艾泰科技
UTT Technologies
www.utt.com.cn

HiPER gv439c4

高级配置手册

上海艾泰科技有限公司

http://www.utt.com.cn

版权声明

版权所有©2000-2005，上海艾泰科技有限公司，保留所有权利。

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0051-001

文档编号（DN）：PR-PMMU-1107.04-PPR-CN-1.0A

目　录

版权声明 **2**

目　录 ..... **I**

导　　读 **1**

0.1　手册说明 1
0.2　界面风格 1
0.3　基本约定 2
0.3.1　列表框详解 2
0.3.2　符号约定 3
0.3.3　表达约定 4
0.4　出厂配置 4
0.5　内容简介 5

第 1 章　产品概述 **7**

1.1　关键特性 7
1.2　主要特点 7
1.3　VPN 功能 9
1.4　规格 9

第 2 章　硬件安装 **10**

2.1　安装准备 10
2.2　安装流程 10
2.3　HiPER 3110 SOHO/3110/2190NBII 安装步骤 11
2.4　HiPER 2231CS/2190NB+安装步骤 13

第 3 章　快速向导 **15**

3.1　配置正确的网络设置 15
3.2　快速向导 16
3.2.1　登录密码设置 17
3.2.2　系统时钟配置 18
3.2.3　上网接入方式设置 18
3.2.4　上网接入线路配置 19
3.2.4.1　PPPoE 拨号上网配置 19
3.2.4.2　固定 IP 接入配置 21
3.2.4.3　动态 IP 接入配置 22

第 4 章　基本配置 **24**

4.1　ISP 配置 24
4.1.1　线路连接信息 24
4.1.1.1　PPPoE 拨号接入时线路连接信息 24
4.1.1.2　固定 IP 接入时线路连接信息 26

4.1.1.3 动态 IP 接入时线路连接信息 27
4.1.1.4 双线路接入时线路连接信息 29
4.1.2 ISP 配置 30
4.1.2.1 PPPoE 拨号上网的配置 31
4.1.2.2 固定 IP 接入的配置 33
4.1.2.3 动态 IP 接入的配置 33
4.1.2.4 删除线路 34
4.2 线路组合 36
4.2.1 线路组合方式 36
4.2.1.1 线路工作机制 36
4.2.1.2 线路检测机制 36
4.2.1.3 线路检测方法 37
4.2.1.4 相关的静态路由 38
4.2.2 线路组合配置 38
4.2.2.1 线路备份 38
4.2.2.2 负载均衡 39
4.2.2.3 配置线路组合 41
4.2.2.4 线路组合配置实例 42
4.2.3 查看双线路状态 43
4.2.4 调度规则配置 44
4.2.4.1 调度规则配置 44
4.2.4.2 自定义调度规则 44
4.2.4.3 调度规则配置实例 45
4.3 DHCP 和 DNS 服务器 46
4.3.1 DHCP 服务配置 46
4.3.2 DHCP 地址池使用信息 47
4.3.3 配置 DHCP 服务器 48
4.3.4 DHCP 手工绑定配置 48
4.3.5 DHCP 手工绑定列表 49
4.3.6 自定义 DHCP 手工绑定 49
4.4 端口配置 50
4.4.1 端口配置 50
4.4.2 配置 IP 地址 50
4.4.3 配置第二个 IP 地址 51
4.4.4 配置 MAC 地址 51
4.4.5 配置以太网工作模式 51
4.5 DDNS 配置 52
4.5.1 申请 DDNS 帐号 52
4.5.2 配置 DDNS 服务 54
4.5.3 DDNS 状态 54
4.5.4 DDNS 验证 55
4.6 时间段配置 57
4.6.1 时间段配置 57
4.6.2 时间段列表 58

4.6.3 自定义时间段.....59
4.6.4 时间段配置实例.....59
第 5 章 系统管理.....62
5.1 管理员配置.....62
5.1.1 WEB 界面管理员配置.....62
5.1.2 管理员信息列表.....63
5.2 时钟管理.....63
5.3 软件升级.....65
5.3.1 显示和保存当前运行软件.....65
5.3.2 软件升级.....65
5.4 配置管理.....67
5.4.1 保存当前配置.....67
5.4.2 恢复备份配置.....67
5.4.3 恢复出厂配置.....67
5.4.4 重新启动设备.....68
5.5 WEB 服务器.....68
5.6 SNMP 配置.....69
5.7 SYSLOG 配置.....70
5.8 远程管理.....71
第 6 章 高级配置.....72
6.1 组管理.....72
6.1.1 工作组配置.....72
6.1.2 工作组列表.....73
6.1.3 自定义工作组.....73
6.1.4 工作组配置实例.....73
6.2 业务管理.....75
6.2.1 业务管理功能介绍.....75
6.2.1.1 工作组、个人用户及 IPSSG 组.....75
6.2.1.2 业务策略的动作.....76
6.2.1.3 业务策略的类型及排列顺序.....76
6.2.1.4 业务策略的执行顺序.....77
6.2.2 业务策略配置.....77
6.2.3 业务管理全局配置.....79
6.2.4 业务策略信息列表.....80
6.2.5 自定义业务策略.....81
6.2.6 业务策略配置实例.....81
6.2.6.1 工作组策略配置实例.....81
6.2.6.2 个人用户策略配置实例.....84
6.2.6.3 源端口的应用实例.....85
6.3 NAT 和 DMZ 配置.....87
6.3.1 NAT 功能介绍.....87
6.3.1.1 NAT 地址空间.....87
6.3.1.2 三种 NAT 类型.....87

6.3.1.3 主线路 NAT 规则和备份线路 NAT 规则 87
6.3.1.4 根据源地址指定优先通道 88
6.3.1.5 根据线路带宽合理分配流量 88
6.3.1.6 两种流量分配规则 89
6.3.1.7 NAT 静态映射 89
6.3.1.8 虚拟服务器（DMZ 主机） 89
6.3.1.9 NAT 规则的执行顺序 90
6.3.2 NAT 全局配置 90
6.3.3 NAT 规则 91
6.3.3.1 NAT 规则配置 91
6.3.3.2 NAT 规则列表 93
6.3.3.3 自定义 NAT 规则 93
6.3.3.4 NAT 规则配置的注意事项 94
6.3.3.5 NAT 规则配置实例 95
6.3.4 NAT 静态映射 99
6.3.4.1 NAT 静态映射配置 99
6.3.4.2 NAT 静态映射列表 100
6.3.4.3 自定义 NAT 静态映射 100
6.3.4.4 NAT 静态映射配置实例 100
6.4 路由配置 103
6.4.1 静态路由简介 103
6.4.1.1 静态路由 103
6.4.1.2 缺省路由 103
6.4.2 系统保留路由 103
6.4.3 静态路由配置 104
6.4.4 路由列表 105
6.4.5 自定义路由 105
6.5 用户管理 107
6.5.1 用户管理功能介绍 107
6.5.1.1 用户管理概述 107
6.5.1.2 用户管理的工作原理 107
6.5.2 IP 和 MAC 绑定用户配置 109
6.5.3 用户管理全局设置 110
6.5.4 用户绑定信息列表 110
6.5.5 自定义 IP 和 MAC 绑定用户 110
6.5.6 配置上网“白名单”和“黑名单” 111
6.5.6.1 配置上网“白名单” 111
6.5.6.2 配置上网“黑名单” 111
6.6 特殊功能 113
6.6.1 快速转发 113
6.6.2 内网主机速率限制 114
6.6.3 虚拟局域网 114
6.6.4 端口镜像 115
6.6.5 端口镜像应用 115

第 7 章　系统状态 116

7.1　用户统计 116
7.2　NAT 统计 118
7.2.1　NAT 状态信息列表 118
7.2.2　NAT 统计信息列表 118
7.3　端口统计 121
7.4　路由和端口信息 122
7.4.1　路由表信息 122
7.4.2　端口信息 125
7.5　系统信息 126
7.5.1　系统版本 126
7.5.2　系统运行时间 126
7.5.3　系统历史记录 127
7.6　系统异常信息 129

第 8 章　上网监控 130

8.1　查询条件 130
8.2　上网监控查询页面 131
8.3　查询实例 132
8.3.1　查询局域网 IP 地址为 200.200.200.198/24 的用户当前上网行为 132
8.3.2　查询局域网内目前访问 www.utt.com.cn 的用户 132
8.3.3　查询局域网内目前使用 MSN 的用户 133
8.3.4　查询局域网内目前使用 WAN2 口 IP 地址上网的信息 133
8.3.5　查询局域网内目前使用主线路上网的信息 134
8.3.6　查询局域网内目前使用备份线路上网的信息 135

第 9 章　带宽业务 136

9.1　带宽管理基本信息配置 136
9.2　带宽管理策略配置 136
9.3　带宽业务列表 137
9.4　自定义带宽业务 138
9.5　带宽业务配置实例 138

附录 A　配置局域网中的计算机 141

附录 B　FAQ 147

1. ADSL 用户如何上网？ 147
2. 固定 IP 接入用户如何上网？ 148
3. 动态 IP（Cable Modem）接入用户如何上网？ 149
4. 如何将 HiPER 恢复到出厂配置? 150
5．如何使用 CLI“急救模式”？ 157
6. 用户管理（IP/MAC 绑定）、工作组与业务管理 162
7．怎样使用 NetMeeting 聊天？ 164
8. 怎样发现使用带宽最大的用户？ 165
9. 怎样诊断蠕虫病毒或者黑客攻击造成的 HiPER 使用异常的故障？ 166

10. 怎样实现允许从外网 ping 广域网端口地址？.....168
附录 C 常用 IP 协议.....170
附录 D 常用服务端口.....171
附录 E 图索引.....175
附录 F 表索引.....179

导　　读

提示：为了达到最好的使用效果，建议将 Windows Internet Explorer 浏览器升级到 6.0 以上版本。相关下载地址为：

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=1E1550CB-5E5D-48F5-B02B-20B602228DE6

0.1　手册说明

本手册适用于 HiPER 早期的几款产品，具体的产品型号及名称如表 0-1 所示：

产品型号	产品名称	硬件平台	WAN 口数量
HiPER 3110SOHO	HiPER 3110 SOHO 智能宽带防火墙	gv 版本	双 WAN 口
HiPER 2231CS	HiPER 2231CS VPN 安全网关	gv 版本	单 WAN 口
HiPER 3110	HiPER 3110 VPN 安全网关	gv 版本	双 WAN 口
HiPER 2190NB+	HiPER 2190NB+宽带智能路由器	gv 版本	单 WAN 口
HiPER 2190NBII	HiPER 2190NBII 高速网吧专用宽带路由器	gv 版本	双 WAN 口

表 0-1 手册适用产品一览表

本手册描述应用于上述产品的 gv439c4 软件版本（ReOS 5.2 软件平台）的特性和功能，提供基于 WEB 界面的配置方法及其步骤。

用户应保证所使用产品的型号及软件版本与本手册所描述对象一致。由于产品版本升级或其它原因，本手册内容会不定期更新。

另外，由于各型号产品软件规格存在一定差异，所有涉及产品规格的问题请咨询上海艾泰科技有限公司技术支持部。

提示：从 WAN 口的数量来看，HiPER 早期产品分为单 WAN 口产品和双 WAN 口产品两大类，具体请参见表 0-1。本手册中，所有与 WAN2/DMZ 口（备份线路）相关的参数、功能、特性及配置描述，仅双 WAN 口产品支持，在手册其他地方不再特别指出。

0.2　界面风格

WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框　　：选中代表只选用此项功能；

复选框　　：选中代表此选项所述功能被选中；

按钮 ：单击则执行该按钮的动作；

文本框 ：输入相关参数；

列表框 ：通过列表可以找到可供选择的选项；

下拉框 ：通过下拉列表可以找到可供选择的选项。

0.3 基本约定

0.3.1 列表框详解

WEB 界面中的列表框有可编辑列表和只读列表两种类型，下面分别举例进行说明：

1. 可编辑列表

可编辑列表用来显示、编辑各种配置信息，能够编辑、删除列表中的选项，此处以“ DHCP 手工绑定列表 ”（如表 0-2）为例说明可编辑列表中各参数的含义。

表 0-2 DHCP 手工绑定信息列表

1/1 ：当前页面序号/总页面数，此处指第一页/共一页；

第一页 ：超链接，单击即可转到第一页；

上一页 ：超链接，单击即可转到上一页；

下一页 ：超链接，单击即可转到下一页；

最后页 ：超链接，单击即可转到最后页；

前往 第 [ ] 页：超链接，单击可以转到文本框所填的页面；

2/100 ：当前已设置数目/最多可设置数目，此处指当前已经建立 DHCP 手工地址绑定 2 条/最多可建 100 条；

编辑 ：超链接，单击即可进入相应编辑框；

☐ 全选 / 全不选 ：选中后（方框中出现“√”），当前页面所有列表项全部被选中；全选情况下，再单击该方框（方框变为空），当前页面所有列表项全部未被选中；

删除：先选择某条（或多条）需要删除的列表项（单击其首列中的方框，方框中出现“√”，表示选中），再单击“删除”按钮，即可删除选中的列表项。

2. 只读列表

只读列表用来显示系统状态信息，不可编辑，此处以“DHCP 地址池使用信息列表”（如表 0-3）为例说明只读列表中各参数的含义。

表 0-3 DHCP 地址池使用信息列表

1/2、第一页、上一页、下一页、最后页、前往 第 [ ] 页涵义均同前；

2/2：当前显示状态信息数/状态信息总数，此处指当前显示 DHCP 地址池使用信息 2 条/共 2 条。

0.3.2 符号约定

- 表示基本参数，描述参数基本涵义；

  如果界面中该参数前有“*”号，表示该参数为必填项目。例如，如图 0-1 所示，主 DNS 服务器后有“*”号，代表在配置 DNS 服务器时，必须填入主 DNS 服务器 IP 地址。

图 0-1 DNS 服务器配置

表示按钮，描述操作动作；

表示提示，指出重点注意事项。

0.3.3 表达约定

1. 进入某配置界面的表达方式

斜体字***配置界面一名称—>配置界面二名称—>配置界面三名称***表示首先进入“ 配置界面一 ”，然后进入 “ 配置界面一 ” 中的 “ 配置界面二 ”，最后进入 “ 配置界面二 ” 中的 “ 配置界面三 ”。

例如，***WEB 管理界面—>系统管理—>时钟管理***表示首先进入 “ WEB 管理界面 ”，然后进入 “ WEB 管理界面 ” 中的 “ 系统管理 ” 界面，最后进入 “ 系统管理 ” 界面中的 “ 时钟管理 ” 界面。

2. 进行某动作的表达方式

单击 “ 按钮名 ” 按钮，表示进行该按钮所对应的操作，在本手册中通过在按钮名称上加引号的方式来表示 WEB 界面中的相应操作按钮。例如单击 “ 删除 ” 按钮，就表示进行相应的删除操作，“ 删除 ” 对应按钮 。

3. 选中某选项的表达方式

选中 “ 选项名 ” 选项，表示选中该选项所对应的功能，在本手册中通过在选项名称上加引号的方式来表示 WEB 界面中的相应选项。例如选中 “ 启用快速转发 ” 选项，就表示快速转发功能被启用了，如图 0-2 所示。

图 0-2 启用快速转发

0.4 出厂配置

1. 端口出厂配置如表 0-4 所示：

端口类型	IP 地址	子网掩码
LAN 口	192.168.16.1	255.255.255.0
WAN 口	192.168.17.1	255.255.255.0
DMZ/WAN2 口	192.168.18.1	255.255.255.0

表 0-4 端口出厂配置

2. 系统管理员的用户名出厂设置为 “ Default ”（区分大小写），出厂密码为空。

0.5 内容简介

本手册主要介绍 HiPER 的各个功能的配置及应用，主要包括：产品概述、硬件安装、快速向导、基本配置、系统管理、高级配置、系统状态、上网监控及带宽业务等。

第 1 部分 产品概述
主要介绍 HiPER 的特点及功能特性。

第 2 部分 硬件安装
主要介绍 HiPER 的安装步骤及注意事项。

第 3 部分 快速向导
主要介绍如何快速安装 HiPER，包括：

- 登录密码设置——设置系统新密码；
- 系统时钟配置——手工设置当前系统时间和日期；
- 上网接入线路配置——快速配置上网主线路（即 WAN 口线路），提供 PPPoE、动态 IP、静态 IP 这三种接入方式。

第 4 部分 基本配置
主要介绍产品的基本功能，包括：

- ISP 配置——配置上网主线路及备份线路，查看线路连接信息；
- 线路组合——配置线路检测方法，选择线路组合方式，设置线路相关参数。配置调度规则，即快速配置静态路由；
- DHCP 和 DNS 服务器——配置 DHCP 服务器、DNS 服务器及 DHCP 手工绑定，查看 DHCP 手工绑定信息以及 DHCP 地址池使用信息；
- 端口配置——配置 HiPER 物理端口的相关参数；
- DDNS 服务——申请、配置 DDNS 服务；
- 时间段配置——配置时间段实例。

第 5 部分 系统管理
主要介绍产品相关管理参数的设置，包括：

- 管理员配置——设置 WEB 管理员，提供三个管理员组：浏览、执行和系统管理；
- 系统时钟管理——手工或自动设置系统时间和日期；
- 设备软件升级——备份当前软件版本，下载最新软件升级；
- 设备配置管理——备份系统当前配置，恢复保存过的配置，恢复设备出厂配置；
- WEB 服务器配置——配置 WEB 服务器相关参数；
- SNMP 配置——配置 SNMP 服务；
- SYSLOG 配置——配置 SYSLOG 服务；
- 远程管理——配置远程管理，允许或禁止远程 HTTP、SNMP 或 TELNET 服务、

第 6 部分 高级配置
主要介绍产品的高级功能配置，包括：

- 组管理——定义局域网用户工作组，具有类似性质（如上网要求相同）的用户划分在同一个工作组；
- 业务管理——定义局域网工作组用户及个人用户的业务策略，从而按要求控制局域网用户的上网行为；

- NAT 和 DMZ 配置——配置 NAT 规则、DMZ 服务器、NAT 静态映射，查看 NAT 规则列表、NAT 静态映射列表。HiPER 提供 EasyIP、One2One 及 Passthrough 三种类型的 NAT 规则，支持配置多条 NAT 规则、多个 DMZ 服务器；
- 路由配置——配置静态路由，预先指定对某一网络访问时所要经过的路径；
- 用户管理——配置 IP/MAC 绑定，防止 IP 地址盗用，配置上网“黑名单”和“白名单”；
- 特殊功能——配置快速转发、内网主机速率限制、虚拟局域网及端口镜像。

第 7 部分 系统状态

主要介绍如何查看系统相关状态信息，包括：

- 用户统计信息——查看局域网用户的上传和下载数据包的统计信息；
- NAT 统计信息——查看针对 NAT 的局域网主机的特别信息，用以发现用户在使用 Internet 过程中发生的 DDoS 攻击、巨量下载、过分占用 Internet 带宽等情况；
- 端口统计信息——查看 HiPER 端口的统计信息，比如接收、转发数据包的速率，经各端口数据包的统计等；
- 路由和端口基本信息——查看当前使用的路由信息，查看端口配置及工作状态；
- 系统信息——查看系统的版本信息、运行时间及历史记录等；
- 系统异常信息——查看系统的异常信息，HiPER 在运行中发生的一些错误会在这里生成相关记录。

第 8 部分 上网监控

主要介绍如何监控局域网用户的上网状况，可以根据主线路、备份线路、源地址、目的地址、域名、NAT 地址、目的端口、以及全部记录等条件查询局域网用户的上网情况。

第 9 部分 带宽业务

主要介绍产品的带宽业务功能，通过设置局域网各用户工作组应用带宽的大小和优先级，将 ISP 分配的带宽二次分配给各工作组。

第 10 部分 附录

本手册共提供 6 个附录，描述如下：

- 附录 A 配置局域网中计算机——提供配置局域网计算机的 TCP/IP 属性的方法。
- 附录 B FAQ——提供常见问题解答；
- 附录 C 常用 IP 协议号——提供常用 IP 协议号与协议名对照表；
- 附录 D 常用服务端口号——提供常用服务端口号及服务名对照表；
- 附录 E 图索引——提供本手册所有图的索引目录；
- 附录 F 表索引——提供本手册所有表的索引目录。

提示：对于 HiPER 2231CS 和 HiPER 3110 两款 VPN 安全网关产品来说，有关 VPN 配置部分请查阅随机附带光盘中的《HiPER VPN 安全网关 VPN 配置手册》（注意，仅 VPN 安全网关产品支持），也可登录艾泰科技官方网站 http://www.utt.com.cn 下载相关配置手册。

第1章　产品概述

非常感谢您选用上海艾泰科技有限公司的 HiPER 系列宽带路由器/防火墙/VPN 安全网关产品。

本章主要讲述 HiPER 早期的几款产品的功能和特点。

1.1　关键特性

- 多端口 10/100Mbps 交换机（MDI/MDI-X 自适应，注：需要网卡或者交换机端口支持，下同）
- 10/100M 自适应 WAN 口（MDI/MDI-X 自适应）
- 10/100M 自适应 DMZ/WAN2 口（MDI/MDI-X 自适应）
- 共享 Internet 接入（ADSL、Cable Modem、以太网接入）
- WEB 界面实时监控、管理局域网内的流量和用户
- 基本防火墙功能
- 防止 DoS/DDoS 攻击
- 支持双 WAN 口流量负载均衡以及线路备份
- 基于 IP 地址和 MAC 地址的多种策略的业务管理
- 独有的基于 CBQ 技术的带宽分配和管理
- 支持快速转发
- 支持内网主机速率限制
- 支持基于端口的 VLAN
- 支持端口镜像

1.2　主要特点

1. 局域网端口（LAN）

- 多端口交换机：集成了多端口 10/100Mbps 自适应交换机（MDI/MDI-X 自适应）。
- 支持 DHCP Server：Dynamic Host Configuration Protocol（动态主机分配协议）可以　给局域网中的计算机动态分配 IP 地址以及网关、DNS Server 等信息。HiPER 可以为局域网提供 DHCP Server 的服务。
- 支持多网段：支持静态路由和动态路由（RIP I，RIP II），可以连接多个不同的网段。
- 基于端口的 VLAN：一个 VLAN 组成一个逻辑子网，即一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信；不同的 VLAN 之间实现物理隔离。
- 端口镜像：LAN 口的端口 1 为镜像端口，可将其他端口的流量自动复制到镜像端口，实时提供各端口的传输状况的详细资料，以便网络管理人员进行流量监控、性能分析和故障诊断。

2. 广域网端口（WAN）

- 广域网端口（WAN）：集成了 10/100Mbps 自适应端口（MDI/MDI-X 自适应）。
- 共享 Internet 访问 :所有的局域网用户可以通过 NAT（Network Address Translation）共享一条 Internet 线路上网。
- 支持 DSL 或者 Cable Modem：HiPER 系列产品通过了和市场上众多厂商的 DSL Modem 和 Cable Modem 的兼容性测试。
- 支持 PPPoE：支持使用 PPPoE（PPP over Ethernet）协议和 ISP 连接。
- 支持固定&动态 IP 地址：支持在使用以太网接入（FTTX+LAN）时，使用固定的和动态的 IP 地址。
- DMZ/WAN2 端口：集成了 10/100Mbps 自适应端口（MDI/MDI-X 自适应）；支持独立的 DMZ 网段；和 WAN 口配合，支持双 WAN 口流量负载均衡以及线路冗余备份。

3. 用户管理和业务控制

- 支持 IP 地址和 MAC 地址绑定。
- 支持多种 Internet 业务的管理与控制。
- 支持 Internet 不良地址过滤。
- 支持分时间段控制上网。

4. IP QoS 功能（基于 CBQ 算法）

- 根据用户传输流的 IP 地址提供不同的带宽分配与管理。
- 根据用户传输流的协议提供不同的带宽分配与管理。
- 根据用户传输流的应用类型提供不同的带宽分配与管理。

5. 配置和管理

- 简易配置：提供 Web UI 和 CLI（命令行）两种配置界面，方便管理和配置。
- 快速安装向导：使用快速安装向导可以非常简单快速的实现和 Internet 的连接。
- 远程管理：在局域网或者广域网上的任何一台计算机上均可实现对 HiPER 的远程管理。

6. Internet 高级特性

- 虚拟服务器（DMZ 主机）：支持配置多台 DMZ 主机，DMZ 主机将完全暴露在 Internet 上，方便远程用户访问。
- NAT 静态映射：支持用户自定义多条 NAT 静态映射，方便远程用户访问内部服务器提供的服务端口。
- 特殊应用程序支持：支持一些特殊的 Internet 应用程序（例如腾讯 QQ、网络游戏、视频程序、音频程序）的使用。
- DDNS：支持动态域名（DDNS）服务。
- 快速转发：可以实现各个物理端口数据的快速转发，全面提高性能。
- 内网主机速率限制：通过控制内网主机上传和下载速率，来实现流量控制。

7. 安全特性

- 配置文件：设置管理员口令，可以防止未被授权的用户修改 HiPER 的配置。备份配置文件，可以防止配置的意外丢失。

- 访问控制：管理员可以限制局域网中的某些用户对 Internet 或者是 Internet 某些服务的访问。
- 实时监控：管理局域网内的流量和用户，及时发现网络异常以及异常用户。
- 防火墙保护：HiPER 可监控所有来自 Internet 的包，过滤所有对局域网内服务器的非法请求，过滤黑客软件对局域网 IP 地址和端口的扫描，以防止外来的恶意攻击。防止 DoS/DDoS 攻击。

1.3 VPN 功能

此外，HiPER VPN 安全网关系列产品提供全面的 VPN 功能，支持 L2TP VPN 和 PPTP VPN，它们还可结合使用。

- 支持使用动态地址构建 VPN 隧道
- 可实现网关到网关的 VPN
- 可实现远程拨号的 VPN
- L2TP/PPTP 服务器
- L2TP/PPTP 客户端

1.4 规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由、RIPI/II、SNMP（MIB II）等协议。
- 端口支持自动协商功能，自动调整传输方式和传输速度。
- 端口支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃
  高度：0-4000m
  相对湿度：10-90%，不结露

第2章 硬件安装

本章主要讲述如何安装 HiPER 系列产品及注意事项，包括：HiPER 3110 SOHO 智能宽带防火墙、HiPER 2231CS VPN 安全网关、HiPER 3110 VPN 安全网关、HiPER 2190NB+宽带智能路由器以及 HiPER 2190NBII 高速网吧专用宽带路由器等。

其中，HiPER 3110 SOHO、HiPER 3110 和 HiPER 2190NBII 的外观及安装步骤类似，HiPER 2231CS 和 HiPER 2190NB+的外观及安装步骤也类似，因此将它们分别放在一起介绍。

2.1 安装准备

1. 10/100M 以太网和 TCP/IP 协议。
2. 准备 DSL 或者 Cable Modem，并从 ISP 那里获得访问 Internet 的用户名和密码。

2.2 安装流程

在安装 HiPER 之前，必须保证 HiPER 的电源是关闭的。HiPER 系列产品的安装流程基本一致，一般经过以下几个步骤：

第一步，选择安装地点，一般是将 HiPER 安装在工作台上。如果是 HiPER 3300NB 或 HiPER 3300VF，还可根据需要将其安装在标准机架上。

第二步，建立 HiPER 与局域网的连接，即将管理计算机或交换机连接到 HiPER 的局域网端口。

第三步，建立 HiPER 与广域网的连接，即将 Cable/DSL Modem 连接到 HiPER 的广域网端口。

第四步，打开电源，打开电源之前确保电源供电、连接、接地正常。

第五步，检查系统指示灯，查看 HiPER 的连接及工作状态是否正常。

以下各节将分别介绍各型号产品的安装步骤、接线图及指示灯状态。

2.3 HiPER 3110 SOHO/3110/2190NBII 安装步骤

1. 选择安装地点

选择一个适当的地方安装 HiPER 3110 SOHO/3110/2190NBII，确保 HiPER 和 Cable/DSL Modem 的电源是关闭的。

2. 连接 HiPER 3110 SOHO/3110/2190NBII 到管理计算机或局域网

使用标准的网线连接管理计算机到 HiPER 3110 SOHO/3110/2190NBII 的局域网（LAN）口，或者是连接你的交换机到 HiPER 的 LAN 口，如图 2-1 所示。HiPER 将会自动适应 10M 或者是 100M 的设备。

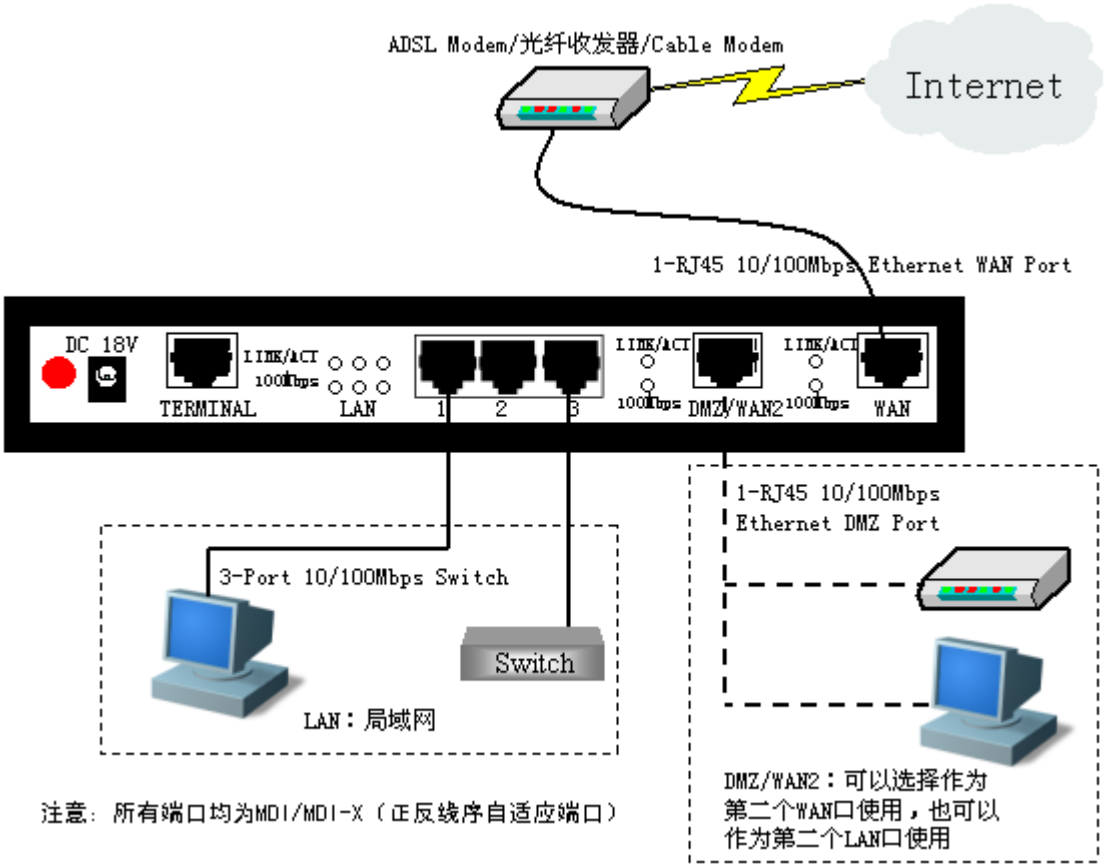


图 2-1 建立局域网和广域网连接——HiPER 3110 SOHO/3110/2190NBII

3. 连接 HiPER 3110 SOHO/3110/2190NBII 到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 3110 SOHO/3110/2190NBII 的广域网（WAN）口，如图 2-1 所示。如果没有厂商提供的网线，请使用标准网线。

4. 打开电源

将随机配置的直流电源适配器连接到 HiPER 3110 SOHO/3110/2190NBII（连接到背板的电源接口），然后将电源线接到合适的插座上。

注意！连接电源之前确保电源供电、连接、接地正常，并使用随机提供的 220V 交流-直流变压器，否则可能造成系统工作异常或系统损坏。

5. 检查系统指示灯

1) 前面板（面向操作者方向）

前面板共有 5 个指示灯，如图 2-2 所示，各指示灯的具体状态如表 2-1 所示。

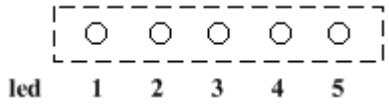


图 2-2 前面板指示灯示意图——HiPER 3110 SOHO/3110/2190NBII

指示灯	启动时状态	启动后状态
led1（wan）	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁
led2（sys）	启动时 led1（wan）熄灭时闪烁一下后常灭	常灭
led3（act）	常灭	常灭
led4（lan）	灭	常亮，有网络流量时闪烁
led5（pwr）	常亮	常亮

表 2-1 前面板指示灯状态——HiPER 3110 SOHO/3110/2190NBII

2) 后面板（面向操作者方向）

后面板共有 5 对指示灯（2 行 5 列，共 10 个），如图 2-3 所示，各指示灯的具体状态如表 2-2 所示。

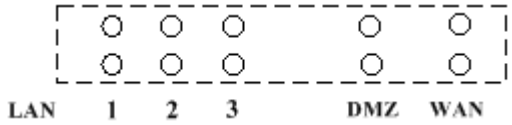


图 2-3 后面板指示灯示意图——HiPER 3110 SOHO/3110/2190NBII

指示灯	启动时状态	启动后状态
上排灯（LINK/ACT）	上排灯闪烁后熄灭（DMZ 灯始终熄灭）	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁
下排灯（100Mbps）	上排灯熄灭后，下排灯闪烁后熄灭（DMZ 灯始终熄灭）	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯长亮

表 2-2 后面板指示灯状态——HiPER 3110 SOHO/3110/2190NBII

2.4 HiPER 2231CS/2190NB+安装步骤

1. 选择安装地点

选择一个适当的地方安装 HiPER 2231CS/2190NB+，确保 HiPER 和 Cable/DSL Modem 的电源是关闭的。

2. 连接 HiPER 2231CS/2190NB+到管理计算机或局域网

使用标准的网线连接管理计算机到 HiPER 2231CS/2190NB+的局域网（LAN）口，或者是连接你的交换机到 HiPER 的 LAN 口，如图 2-4 所示。HiPER 将会自动适应 10M 或者是 100M 的设备。

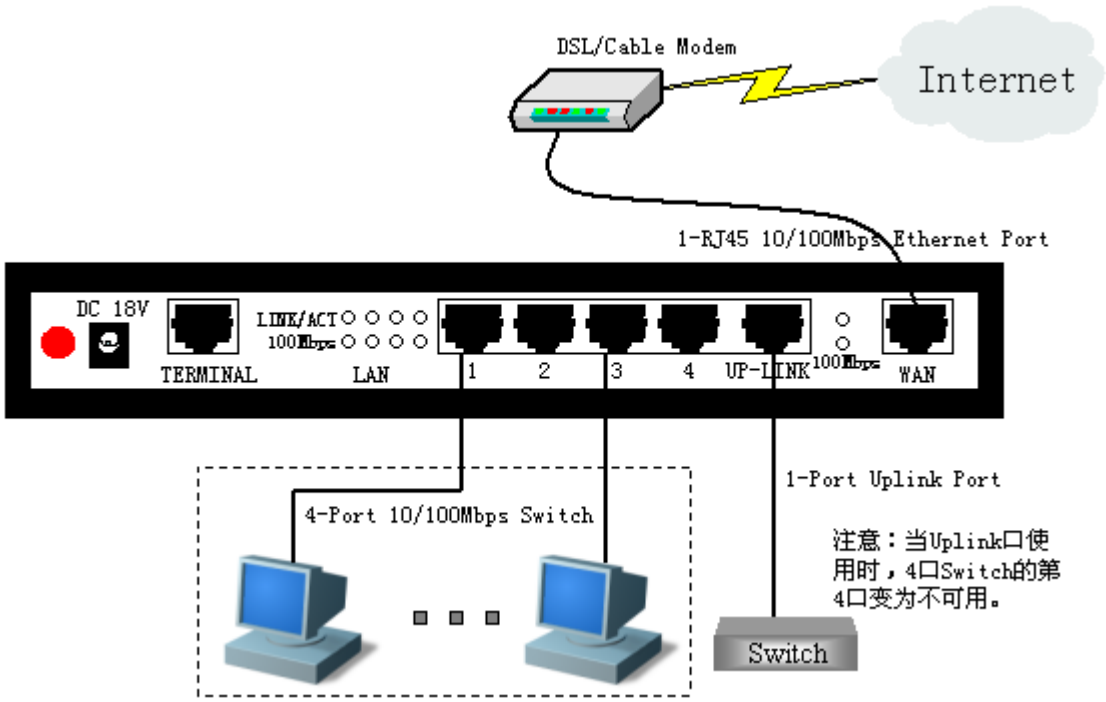


图 2-4 建立局域网和广域网连接——HiPER 2231CS/2190NB+

3. 连接 HiPER 2231CS/2190NB+到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 2231CS /2190NB+的广域网（WAN）口，如图 2-4 所示。如果没有厂商提供的网线，请使用标准网线。

4. 打开电源

连接随机配置的直流电源适配器到 HiPER 2231CS/2190NB+（连接到背板的电源接口），然后将电源线接到合适的插座上。

注意！连接电源之前确保电源供电、连接、接地正常，并使用随机提供的 220V 交流-直流变压器，否则可能造成系统工作异常或系统损坏。

5. 检查系统指示灯

1) 前面板（面向操作者方向）

前面板共有 5 个指示灯，如图 2-5 所示，各指示灯的具体状态如表 2-3 所示。

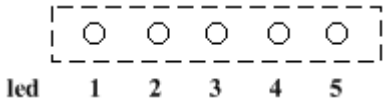


图 2-5 前面板指示灯示意图——HiPER 2231CS/2190NB+

指示灯	启动时状态	启动后状态
led1（wan）	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁；系统负担较大时，闪烁频率降低
led2（sys）	启动时 led1（wan）熄灭时闪烁一下后常灭	常灭
led3（act）	常灭	常灭
led4（lan）	灭	常亮，有网络流量时闪烁
led5（pwr）	常亮	电源工作正常时常亮

表 2-3 前面板指示灯状态——HiPER 2231CS/2190NB+

2) 后面板（面向操作者方向）

后面板共有 5 对指示灯（2 行 5 列，共 10 个），如图 2-6 所示，各指示灯的具体状态如表 2-4 所示。

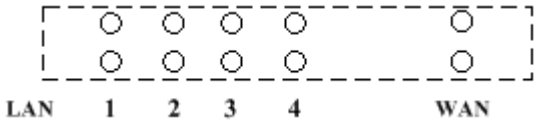


图 2-6 后面板指示灯示意图——HiPER 2231CS/2190NB+

指示灯	启动时状态	启动后状态
上排灯（LINK/ACT）	上排灯闪烁后熄灭	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁
下排灯（100Mbps）	上排灯熄灭后，下排灯闪烁后熄灭	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯长亮

表 2-4 后面板指示灯状态——HiPER 2231CS/2190NB+

第3章　快速向导

使用 HiPER 之前，首先要对计算机进行合理的网络配置并对 HiPER 进行最基本的配置。通过阅读本章内容，可以设置路由器上网所需的基本网络参数，快速的将 HiPER 连接到 Internet。

3.1　配置正确的网络设置

HiPER 的局域网端口的出厂配置为：IP 地址是 192.168.16.1，子网掩码是 255.255.255.0。这些参数可以根据实际需要而改变，本手册均按出厂值说明。

首先将计算机连接到 HiPER 的局域网端口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，请参考附录 A。如果已经正确设置完成，请跳过此步。

第二步，设置计算机的 IP 地址为 192.168.16.2-192.168.16.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.16.1，DNS 服务器为当地运营商提供的地址。

第三步，使用 Ping 命令检查计算机和 HiPER 之间是否连通。下面的例子是在 Windows XP 环境中，执行 Ping 命令：**Ping 192.168.16.1**

如果屏幕显示如下，表示计算机已经成功和 HiPER 建立连接。

```
Pinging 192.168.16.1 with 32 bytes of data:

Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

如果屏幕显示如下，表示计算机和 HiPER 连接失败。

```
Pinging 192.168.16.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

连接失败时，请做以下检查：

1. 硬件连接：HiPER 面板上与局域网端口对应的 LINK/ACT 指示灯和计算机上的网卡灯必须亮。

2. 计算机 TCP/IP 属性的配置：如果 HiPER 的 IP 地址为 192.168.16.1，那么计算机的 IP 地址必须为 192.168.16.2-192.168.16.254 中的任意一个空闲地址。

3.2　快速向导

本节讲述 ***WEB 管理界面—>基本配置—>快速向导***页面的配置。

计算机如果是使用 MS Windows、Macintosh、Unix 或者是 Linux 等任何操作系统，都可以通过浏览器（Internet Explorer 或 Netscape Communicator）来对 HiPER 进行配置。

打开浏览器，在浏览器的地址栏里输入 HiPER 的 IP 地址，例如 http://192.168.16.1。

连接建立起来之后，将会看到如图 3-1 所示的登录界面。首次使用时需要以系统管理员的身份登录，即在该登录界面输入系统管理员的用户名和密码（用户名的出厂设置为“ Default ”，密码的出厂设置为空），然后单击“ 确定 ”按钮。

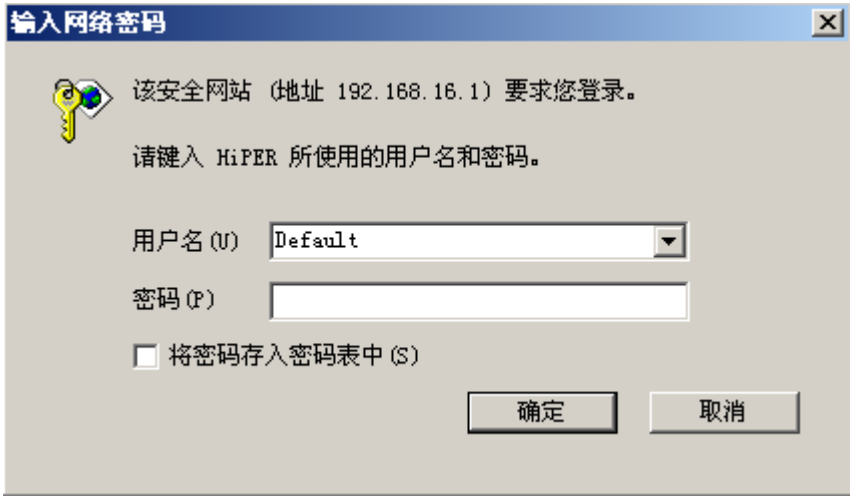


图 3-1 HiPER 登录界面

如果用户名和密码正确，浏览器将显示管理员模式的主页面，该页面右上角显示系统型号及版本信息，如图 3-2 所示。

图 3-2 WEB 界面首页

单击“ 进入 ”按钮，进入“ 快速向导 ”设置界面。快速向导提供配置 HiPER 的最基本功能，如登录密码、系统时钟、主线路接入等。

3.2.1 登录密码设置

HiPER 出厂的管理员（Default）密码为空，建议修改 HiPER 管理员密码并妥善保管，以提高 HiPER 的安全性。修改管理员密码后，以 Default 身份登录 HiPER，必须使用新的密码，如图 3-3 所示。

图 3-3 登录密码设置

- 新密码：登录密码；
- 重复确认：登录密码（此处必须和上一栏所填密码一致）；
- 重填：恢复到修改前的密码；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第二页。

提示：输入密码和确认密码必须一致。请妥善保管新密码，并且不要轻易告诉别人。如果丢失密码，将不能登录 HiPER，必须将 HiPER 恢复到出厂配置（可在 ***WEB 管理界面—>系统管理—>配置管理—>恢复出厂配置***〈章节 5.4.3〉中配置）。

3.2.2 系统时钟配置

在修改登录密码页面中，单击“ 下一步 ”按钮，进入修改系统时钟页面（如图 3-4），在这里可以配置系统日期与系统时间。

图 3-4 系统时钟设置

- 系统日期：当前日期，单位为年、月、日；
- 系统时间：当前时间，单位为时、分、秒；
- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的系统日期和时间；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第三页。

提示：

1. 请正确设置系统时间，HiPER 提供了 DDNS 功能（参见 ***WEB 管理界面—>基本配置—>DDNS 配置***〈章节 4.5〉）和上网时间段管理功能（参见 ***WEB 管理界面—>基本配置—>时间段配置***〈章节 4.6〉），如果时间设置不正确，将导致 DDNS 功能和时间段管理功能不能正常工作；
2. 部分型号没有时间保存功能，在 HiPER 重启后时间会恢复出厂值。这种情况下需要到 ***WEB 管理界面—>系统管理—>时钟管理***（章节 5.2）中选择“ 网络时钟同步 ”方式设置时间。

3.2.3 上网接入方式设置

在修改系统时钟页面中，单击“ 下一步 ”按钮，进入主线路接入方式设置页面（如图 3-5）。HiPER 支持以下三种常用的上网方式，可以根据实际情况进行选择。

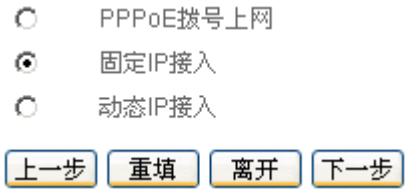


图 3-5 上网接入方式设置

- PPPoE 拨号上网：ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号）；
- 固定 IP 接入：以太网宽带接入方式，ISP（例如中国电信）提供静态的 IP 地址；
- 动态 IP 接入：以太网宽带或者有线通接入方式，ISP（例如中国电信）通过 DHCP 服务为用户分配 IP 地址。
- 上一步：返回到快速向导的第二页；
- 重填：恢复到修改前的主线路接入方式；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；

- 选中“ PPPoE 拨号上网 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页 PPPOE 拨号页面；
- 选中“ 固定 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页固定 IP 接入页面；
- 选中“ 动态 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页动态 IP 接入页面。

3.2.4 上网接入线路配置

3.2.4.1 PPPoE 拨号上网配置

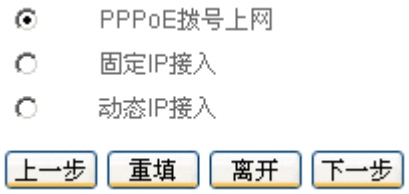


图 3-6 PPPoE 拨号上网方式

在选择主线路接入方式页面中，选中“ PPPoE 拨号上网 ”选项，如图 3-6 所示。单击“ 下一步 ”按钮，进入 PPPoE 配置页面（如图 3-7），配置 PPPoE 信息，单击“ 保存 ”按钮，PPPoE 主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1. 如果改变了 HiPER 的“ 局域网 IP 地址 ”，在完成本向导之后，必须使用新的 IP 地址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网；

2. 如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1）中检查线路状态，查看、修改配置参数。

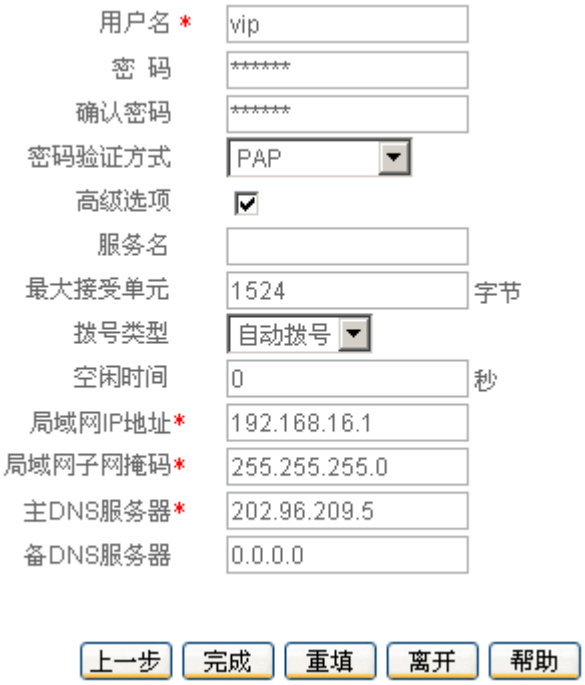


图 3-7 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码（如有疑问，请询问 ISP）；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置（如有疑问，请询问 ISP）；
- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式（如有疑问，请询问 ISP）；
- 最大接受单元：缺省值为 1524 字节，PPPoE 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：
  自动拨号：当开启 HiPER 或者上一次拨号断线后自动拨号连接；
  手动拨号：在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中手动进行连接和挂断；
  按需拨号：在局域网内部有访问 Internet 流量时 HiPER 自动进行连接；
- 空闲时间：在没有访问 Internet 流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的 PPPoE 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。
- 提示：所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

3.2.4.2　固定 IP 接入配置

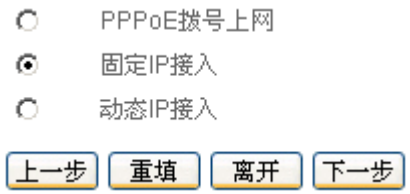


图 3-8 固定 IP 接入方式

在选择主线路接入方式页面中，选中“固定 IP 接入”选项，如图 3-8 所示。单击“下一步”按钮，进入固定 IP 接入页面（如图 3-9），在这里配置固定 IP 接入信息，单击“保存”按钮，固定 IP 接入主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1. 如果改变了“局域网 IP 地址”，在完成本向导之后，必须使用新的 IP 地址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网；
2. 如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1）中检查线路状态，查看、修改配置参数。

图 3-9 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供 HiPER 使用的广域网 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的固定 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 保存：快速向导运行成功，所做的操作在这里生效。

提示：

1. 所做的操作，只有单击“完成”按钮才生效（包括快速向导的前几页）；
2. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）提供的广域

网 IP 地址和静态网关不在同一网段，请修改子网掩码，使它们在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部。

3.2.4.3　动态 IP 接入配置

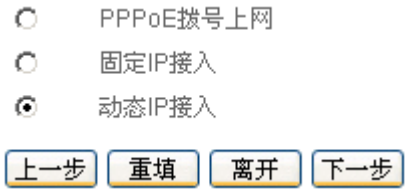


图 3-10　动态 IP 接入方式

在选择主线路接入方式页面中，选中“ 动态 IP 接入 ”选项，如图 3-10 所示。单击“ 下一步 ”按钮，进入动态 IP 接入页面（如图 3-11），在这里配置动态 IP 接入信息，单击“ 保存 ”按钮，动态 IP 接入主线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

提示：

1)　如果改变了“ 局域网 IP 地址 ”，在完成本向导之后，必须使用新的 IP 地址重新登录 HiPER，才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

2)　如果发现完成配置后不能上网，请检查各项配置是否正确，可在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1）中检查线路状态，查看、修改配置参数。

图 3-11　动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网端口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备（这里指 HiPER）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址（可能会在线路刷新时更新成 ISP 分配的地址）；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的动态 IP 配置参数；

- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 保存：快速向导运行成功，所做的操作在这里生效。
- 提示：所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

配置好快速向导后，HiPER 的一些最基本的功能已经配置完成。此时，再根据附录 A 中的内容完成计算机的 TCP/IP 属性的设置，即可进行各种各样的 Internet 操作了。同时还可以在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中，查看线路的配置和状态信息。

第4章　基本配置

HiPER 除提供基本的上网共享功能外，还提供了一些附加的 IP 功能，方便配置、管理网络。本章主要讲述如何设置上网所需的基本网络参数，如 ISP 配置、线路组合、DHCP 服务、DNS 服务器、端口配置、DDNS 服务、时间段配置等。

4.1　ISP 配置

本节主要讲述 ***WEB 管理界面—>基本配置—>ISP 配置***的配置方法。

在本页面不仅可以配置主线路及备份线路，还可以修改和删除已配置的线路。同时，可以在这里查看线路的连接状态信息；如果配置了双线路，可以查看两条线路的的连接状态信息。

通过快速向导以后，可以到这里查看主线路的连接状态和配置情况，也可以根据需要修改主线路配置。在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中修改主线路配置后，这里会自动修改相应参数；同时，在这里修改主线路配置后，在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中也会自动修改相应参数。

4.1.1 线路连接信息

这一节将分别介绍单线路接入（PPPoE 拨号、固定 IP 接入、动态 IP 接入）以及双线路接入时，如何查看线路连接的一些配置和状态信息。

提示：对于单 WAN 口产品，各种接入方式下，“ 线路连接信息 ” 中均不显示 “ 线路连接状态 ” 相关信息。

4.1.1.1　PPPoE 拨号接入时线路连接信息

如果快速向导配置的是 PPPoE 线路，可以在这里查看 PPPoE 拨号接入时的一些配置和状态信息，如图 4-1 所示。在 “ 线路连接状态 ” 中可以查看线路运行状态；在 “ 主线路连接信息 ” 中，“ 连接类型 ” 将显示 “ PPPoE 拨号上网 ”，如果 “ 连接状态 ” 显示 “ 已连接 ”，则可以在 “ 连接类型 ” 下面看到 ISP 分配的 “ IP 地址 ”、“ 子网掩码 ” 以及 “ 使用时间 ” 等信息；在 “ 局域网信息 ” 中可以查看局域网端口相关信息。

图 4-1 PPPoE 拨号时线路连接信息

1. 线路连接状态

- 线路组合方式：当前使用单线路上网；
- 主线路状态：当前线路的运行状态。线路运行正常时显示为“ 主线路运行正常 ”，线路中断时显示为“ 主线路运行异常 ”；
- 备份线路状态：当前无备份线路，始终显示为“ 没有配置备份线路 ”；
- 主线路流量：“ 统计时长 ” 内，线路一直无流量时该值为“ 0% ”，有流量时该值为“ 100% ”；
- 备份线路流量：当前无备份线路，该值始终为“ 0% ”；
- 统计时长：两次刷新本页面的时间间隔（时间单位为天:时:分:秒）。

2. 主线路连接信息

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 8 种状态，详见表 4-1；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
拨号中	拨号已经发起，但是服务方尚未响应
验证中	服务方已经响应，正在验证用户名、密码
已连接	验证通过，PPPoE 连接已经建立，可以传送数据
断线中	正在拆除 PPPoE 连接
已挂机	一方已经发出挂机请求
已断线	PPPoE 连接已中断，等待拨号
内部错误	其它未定义状态

表 4-1 PPPoE 拨号线路连接状态描述

- IP 地址、子网掩码：ISP 当前分配的广域网端口的 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址，在 PPPoE 拨号中该地址与 ISP 当前分配的广域网端口的 IP 地址相同；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前用来 PPPoE 拨号的物理端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 使用时间：该线路保持本次连接的时间（时间单位为天:时:分:秒）。
- 拨号：手动呼叫 PPPoE 连接，拨号过程中，在“连接状态”中可见“已断开”→“拨号中”→“验证中”→“已连接”四个过程。当 PPPoE 连接拨号类型设置为“手动拨号”时，需在这里完成 PPPoE 拨号；
- 挂断：手动挂断 PPPoE 连接，当 PPPoE 连接拨号类型设置为“手动拨号”时，需在这里挂断 PPPoE 连接；
- 刷新：刷新当前页面，获得最新的 PPPoE 拨号线路连接信息（如使用时间等）。

3. 局域网信息

- IP 地址、子网掩码：局域网端口的 IP 地址、子网掩码；
- MAC 地址：局域网端口的 MAC 地址；
- 模式：局域网端口的工作模式。

提示：

1. 当 PPPoE 连接拨号类型设置为“自动拨号”或者“按需拨号”时，此时若 PPPoE 未连接或挂断时，系统会自动拨号或者按流量触发拨号；
2. 刷新后，连接类型下面的 IP 地址就是 PPPoE 拨号当前得到的 IP 地址；
3. 局域网端口以及广域网端口的相关信息可在 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.4）中修改。

4.1.1.2 固定 IP 接入时线路连接信息

如果快速向导配置的是固定 IP 接入线路，可以在这里查看固定 IP 接入时 HiPER 的一些配置和状态信息，如图 4-2 所示。在“线路连接状态”中可以查看线路运行状态；在“主线路连接信息”中可查看主线路相关配置和状态信息，“连接类型”将显示“固定 IP 接入”；在“局域网连接信息”中可查看局域网端口信息。

图 4-2 固定 IP 接入时线路连接信息

“线路连接状态”、“局域网信息”中相关参数的涵义同 PPPoE 拨号接入时相关参数涵义，这里不再重述。

“主线路连接信息”中各参数涵义如下所述：

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 3 种状态，详见表 4-2；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
已连接	物理端口和对方网络设备建立连接
内部错误	其它未定义状态

表 4-2 固定 IP 接入线路连接状态描述

- IP 地址、子网掩码：ISP 提供的广域网端口的静态 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前使用的广域网端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址。
- 刷新：显示最新配置信息。

提示：局域网端口以及广域网端口的相关信息可在 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.4）中修改。

4.1.1.3 动态 IP 接入时线路连接信息

如果快速向导配置的是动态 IP 接入线路，可以在这里查看动态 IP 接入时的一些配置

和状态信息，如图 4-3 所示。在“ 线路连接状态 ”中可以查看线路运行状态；在“ 主线路连接信息 ”中，“ 连接类型 ”将显示“ 动态 IP 接入 ”，如果“ 连接状态 ”显示为“ 已连接 ”，则可以在“ 连接类型 ”下面看到 ISP 分配的“ IP 地址 ”以及“ 剩余租用时间 ”等信息；在“ 局域网连接信息 ”中可查看局域网端口信息。

图 4-3 动态 IP 接入时线路连接信息

“ 线路连接状态 ”、“ 局域网信息 ”中的相关参数的涵义同 PPPoE 拨号接入时相关参数涵义，这里不再重述。

“ 主线路连接信息 ”中各参数涵义如下所述：

- 连接类型：当前上网接入线路的连接类型；
- 连接状态：线路的当前连接状态，共有 4 种状态，详见表 4-4；

连接状态	状态描述
关闭	物理端口没有连接或者路由失效
连接中	正在请求动态的 IP 地址
已连接	已经获得动态分配的 IP 地址，线路连接正常
内部错误	其它未定义状态

表 4-3 动态 IP 接入线路连接状态描述

- IP 地址、子网掩码：ISP 当前分配的广域网端口的 IP 地址、子网掩码；
- 网关地址：默认路由的网关地址；
- MAC 地址：广域网端口的 MAC 地址；
- 物理端口：当前使用的广域网端口；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 剩余租用时间：HiPER 获得 ISP 当前分配的 IP 地址的剩余租用时间（时间单位为天:时:分:秒）。

- 刷新：刷新当前页面，获得最新的动态 IP 链路连接信息；
- 更新：系统自动完成一次先释放 IP 地址、再重新获得 IP 地址的过程（更新过程，在“ 连接状态 ”中可见“ 已断开 ”→“ 连接中 ”→“ 已连接 ”三个过程），更新后主 DNS 服务器可能更新为 ISP 分配的新地址；
- 释放：释放当前得到的动态 IP 地址。

提示：

1. 刷新后，连接类型下面的 IP 地址就是动态 IP 接入当前得到的 IP 地址；
2. 局域网端口以及广域网端口的相关信息可在 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.4）中修改。

4.1.1.4 双线路接入时线路连接信息

如果使用双线路，在这里可以查看双线路接入时的配置和状态信息，如图 4-4 所示，这里以主线路为固定 IP 接入、备份线路为动态 IP 接入为例。在“ 线路连接状态 ”中可以查看两条线路组合方式、运行状态及流量分配情况，在“ 主线路连接信息 ”中可以查看主线路的配置和状态信息，在“ 备份线路连接信息 ”中可以查看备份线路的配置和状态信息，在“ 局域网信息 ”中可以查看局域网端口信息。

图 4-4 双线路接入时线路连接信息

“ 主线路连接信息 ”、“ 备份线路连接信息 ” 以及 “ 局域网信息 ” 中的相关参数涵义与相应单线路接入时相关参数相同，这里不再重述。

“ 线路连接状态 ” 中各参数涵义如下：

- 线路组合方式：双线路接入时，当前使用的线路组合方式，显示为 “ 负载均衡 ” 或 “ 线路备份 ”；
- 主线路状态：当前主线路的运行状态。主线路运行正常时显示为 “ 主线路运行正常 ”，主线路中断时显示为 “ 主线路运行异常 ”；
- 备份线路状态：当前备份线路的运行状态。备份线路运行正常时显示为 “ 备份线路运行正常 ”，备份线路中断时显示为 “ 备份线路运行异常 ”；
- 主线路流量：“ 统计时长 ” 内，主线路流量占线路总流量的百分比；如果 “ 统计时长 ” 内，主线路无流量，该值为 “ 0% ”；
- 备份线路流量：“ 统计时长 ” 内，备份线路流量占线路总流量的百分比；如果 “ 统计时长 ” 内，备份线路无流量，该值为 “ 0% ”；
- 统计时长：两次刷新本页面的时间间隔（时间单位为天:时:分:秒）。

提示：

1. “ 负载均衡 ”、“ 线路备份 ” 这两个参数的具体涵义请参见 ***WEB 管理界面—>基本配置—>线路组合—>线路组合配置***（章节 4.2.2）中相关参数描述；
2. 如果 “ 统计时长 ” 内，两条线路均无流量，“ 主线路流量 ” 和 “ 备份线路流量 ” 均为 “ 0% ”；
3. “ 线路组合方式 ” 为 “ 线路备份 ” 时，若主线路正常，即使备份线路运行正常，“ 备份线路流量 ” 仍为 “ 0% ”；只有主线路故障时，备份线路才会有流量。

4.1.2 ISP 配置

提示：若要使用双线路上网，在本页面配置完主线路和备份线路的相关参数后，可到 ***WEB 管理界面—>基本配置—>线路组合—>线路组合配置***（章节 4.2.2）中配置双线路组合的相关参数。

如果是高级用户，可以不经过快速向导而直接在本界面中配置主线路，同时，也可以配置备份线路。在配置或修改线路前，首先必须配置 “ 选择线路 ” 和 “ 连接类型 ” 这两个参数，如图 4-5 所示。

图 4-5 选择线路和连接类型

- 选择线路：只有配置了主线路之后，才会显示选项 “ 备份线路 ”。
  主线路：欲配置的线路为主线路，主线路通过 WAN 口连接；
  备份线路：欲配置的线路为备份线路，备份线路接通过 WAN2/DMZ 口连接；
- 连接类型：

PPPoE 拨号上网：ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号）；
固定 IP 接入：以太网宽带接入方式，ISP 提供静态的 IP 地址；
动态 IP 接入：以太网宽带或者有线通接入方式，ISP 通过 DHCP 服务为用户分配 IP 地址；
无：用于删除已配置线路。当“ 选择线路 ”为“ 主线路 ”时，可同时删除主线路和备份线路；当“ 选择线路 ”为“ 备份线路 ”时，只删除备份线路。

下面将分别介绍 PPPoE 拨号上网（如图 4-6）、固定 IP 接入（如图 4-7）、动态 IP 接入（如图 4-8）三种情况下线路的详细配置，以及如何删除已配置的线路（如图 4-9、4-12）。这三种情况下，主线路和备份线路的配置界面均相同。

4.1.2.1　PPPoE 拨号上网的配置

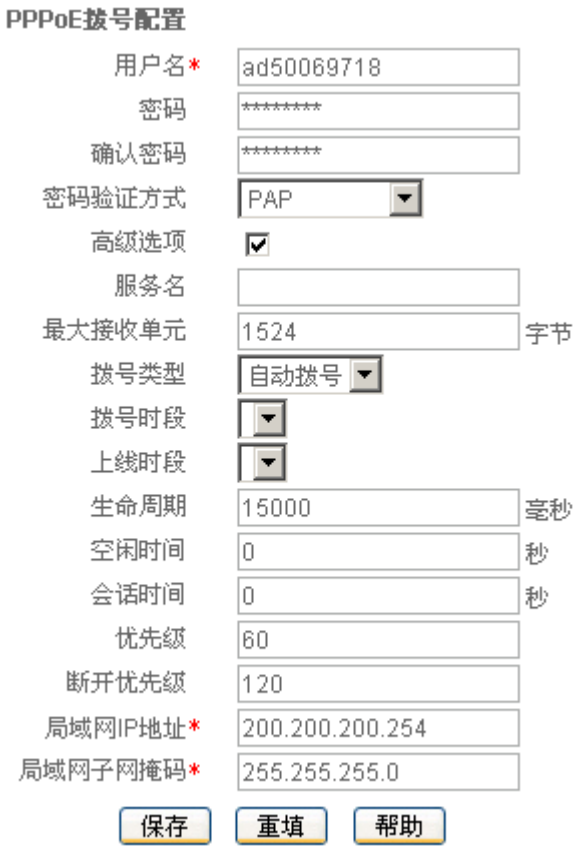


图 4-6 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码。如有疑问，请询问 ISP；
- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置。如有疑问，请询问 ISP；
- 最大接受单元：缺省值为 1524 字节，PPPoE 拨号时路由器将自动与对方设备协商，除非特别应用，不要修改；

- 拨号类型：
  自动拨号：当打开 HiPER 或者上一次拨号断线后自动拨号连接；
  手动拨号：由用户在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中手动进行连接和挂断；
  按需拨号：在局域网内部有访问 Internet 流量时 HiPER 自动进行连接；
- 拨号时段：允许 PPPoE 拨号的时间段（时间段在 ***WEB 管理界面—>基本配置—>时间段配置***〈章节 4.6〉中配置），只有在此时间段内才允许 PPPoE 拨号。不设置代表不对拨号时段进行控制；
- 上线时段：允许 HiPER 上线连接到 Internet 的时间段（时间段在 ***WEB 管理界面—>基本配置—>时间段配置***〈章节 4.6〉中配置），超出这个时间段的范围不允许 HiPER 上线；如果超出时间段时 HiPER 处于连接状态，它将自动断开 PPPoE 连接。不设置代表不对上线时段进行控制；
- 生命周期：在拨号成功后，系统将每隔 300ms 向对端网络设备发送一个探测包，以探测线路是否可用，如果在“ 生命周期 ”范围内一直没有收到对方回应，则断开此连接，默认值：15000 毫秒；
- 空闲时间：在没有访问流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 会话时间：连接生存时间，每次拨号成功到设置的时间后自动断线。一般情况下不要作此设置，0 代表没有时间限制（单位：秒）；
- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 断开优先级：PPPoE 线路断开后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）。
- 保存：PPPoE 接入配置生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 如果改变了“ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网；

2. 与在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）中配置 PPPoE 拨号接入时相关参数相比，这里提供了更多的配置参数，包括：“ 拨号时段 ”、“ 上线时段 ”、“ 生命周期 ”、“ 会话时间 ”、“ 优先级 ”、“ 断开优先级 ” 等，以供高级用户使用。

4.1.2.2　固定 IP 接入的配置

图 4-7 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供 HiPER 对广域网的 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 保存：固定 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）给出的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码的值，使它们处在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部；
2. 如果改变了“局域网 IP 地址”,在保存之后,必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

4.1.2.3　动态 IP 接入的配置

图 4-8 动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；

- 广域网端口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获 IP 地址的现象，此时需要将新的网络设备（这里指 HiPER）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址，在线路刷新时可能会更新成 ISP 分配的新地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 保存：动态 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。

提示：如果改变了“局域网 IP 地址”，在保存之后，必须使用新的 IP 地址重新登录 HiPER 才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

4.1.2.4　删除线路

在这里可以删除已配置的线路，用户可以根据需要删除主线路、备份线路。

提示：

1. 删除线路后，本页面相关配置会恢复到出厂值，需重新配置相关功能，以保证 HiPER 正常工作；

2. 删除线路后，绑定在该线路上的调度规则（在 ***WEB 管理界面—>基本配置—>线路组合—>调度规则配置***〈章节 4.2.4〉中配置）和静态路由（在 ***WEB 管理界面—>高级配置—>路由配置—>路由参数设置***〈章节 6.4.1〉中配置）也被删除。如果需要相应功能，需重新配置；

3. 如果是远程登录配置 HiPER，删除主线路后，系统远程管理功能（在 ***WEB 管理界面—>系统管理—>远程管理***〈章节 5.8〉中配置）将被删除，从而导致到 WAN 口的连接中断。如果需要相应功能，需重新配置。

1. 删除全部线路

如图 4-9 所示，“选择线路”选择为“主线路”，“连接类型”选择为“无”，再单击“保存”按钮，即可删除全部线路。

图 4-9 删除主线路（和备份线路）

如果只配置了主线路，单击“保存”按钮后，将弹出如图 4-10 所示对话框，单击“确定”按钮后，主线路被删除；如果配置了双线路，单击“保存”按钮后，将弹出如图 4-11

所示对话框，单击“ 确定 ”按钮后，主线路和备份线路同时被删除。

图 4-10 对话框——删除主线路

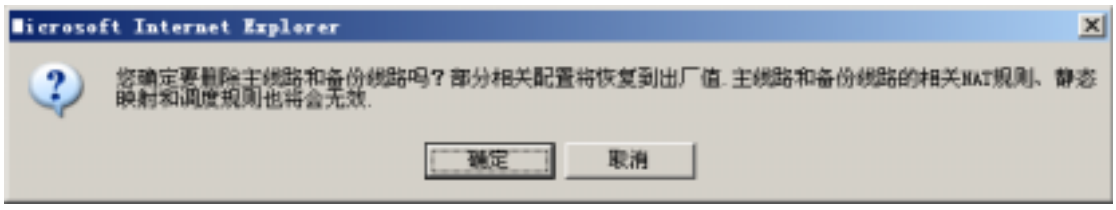


图 4-11 对话框——删除主线路和备份线路

2. 删除备份线路

如图 4-12 所示，“ 选择线路 ”选择为“ 备份线路 ”，“ 连接类型 ”选择为“ 无 ”，再单击“ 保存 ”按钮后，将弹出如图 4-13 所示对话框，单击“ 确定 ”按钮后，备份线路被删除。

图 4-12 删除备份线路

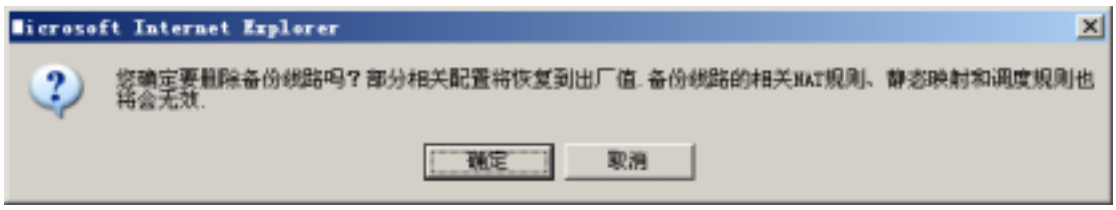


图 4-13 对话框——删除备份线路

4.2　线路组合

本节主要讲述 ***WEB 管理界面—>基本配置—>线路组合***的配置方法，相关功能仅双 WAN 口产品支持。

提示：只有在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）中配置了主线路和备份线路之后，才能进入本页面配置线路组合的相关参数。

本页面由线路组合和调度规则配置两部分组成：

在线路组合配置中，可以快速配置双线路上网的线路组合方式及其他相关参数，可以指定两条线路的线路检测方式，还可以为指定范围内的主机限制上网线路，并能通过不同的分配规则来控制线路流量。

在调度规则配置中，可以为到固定目的地址的路由指定线路（主线路或备份线路）。

4.2.1 线路组合方式

4.2.1.1　线路工作机制

HiPER 中，有线路备份和负载均衡这两种线路组合方式。其中，通过 WAN 口接入的线路为主线路，通过 WAN2/DMZ 口接入的线路为备份线路。

线路备份方式下，主线路正常时，只有主线路工作，局域网内所有主机都通过主线路上网；当主线路出现故障时，立即被屏蔽，并自动切换到备份线路；一旦主线路恢复正常，立即自动切换回主线路。

负载均衡方式下，线路正常时，局域网内主机同时使用两条线路上网；若某条线路出现故障，该线路将被屏蔽，原先经该线路的流量将分配到另外那条线路，即局域网内所有主机都通过正常的那条线路上网；一旦故障线路恢复正常，HiPER 会自动启用该线路，流量重新分配到两条线路。

提示：当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP 会话的属性决定的。艾泰科技将不承担由此引发的一切用户损失或者法律诉讼。

4.2.1.2　线路检测机制

不论是线路备份，还是负载均衡方式下，要保证线路故障时网络不中断，都要求 HiPER 必须能够实时地监控线路状态。为此，我们为 HiPER 设计了灵活的自动检测机制，并提供多种线路检测方法供用户选择，以满足实际应用的需要。

为方便理解，先介绍一下几个相关参数。

检测目标：检测的目标对象，HiPER 将向预先指定的检测目标发送检测包以检测线路是否正常。

检测间隔：发送检测包的时间间隔，一次发送一个检测包，缺省值为 1000 毫秒。该值为 0 时，表示不进行线路检测。

检测次数：发送检测包的次数，即检测包的数量，缺省值为 3 次。

检测周期：该值为检测间隔与检测次数的乘积，例如，缺省情况下，该值为 1000×3

＝3000 毫秒。

下面将分别介绍在线路正常和线路故障这两种情况下，HiPER 的线路检测机制。

线路正常时，检测机制如下所述：HiPER 将每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的所有检测包都没有回应，就认为该线路出现故障，并立即屏蔽该线路。例如，缺省情况下，若某个检测周期内，发送的 3 个检测包都没有回应，就认为该线路出现故障。

线路故障时，检测机制如下所述：同样地，HiPER 也是每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的检测包中有一半及以上数量的检测包有回应时，就认为该线路已经正常，并恢复启用该线路。例如，缺省情况下，若某个检测周期内，有 2 个检测包有回应，就认为该线路恢复正常。

提示：允许不启用线路检测，这时需要将“检测间隔”设为“0 毫秒”。

4.2.1.3　线路检测方法

HiPER 支持三种线路检测方法：ICMP、ARP 及 DNS，用户可选择其中的一种来监控两条线路的状态，注意：两条线路只能使用相同的检测方式，但可设置不同的检测参数。各方式具体描述如下：

- ICMP 方法：HiPER 向检测目标发送 ICMP 检测包，以检测线路是否激活。此方法中，检测目标的缺省值为网关地址，用户也可以自定义其他欲检测的目标地址；
- ARP 方法：HiPER 向网关发送 ARP 检测包，以检测线路是否激活。此方法中，检测目标只能为网关地址，不能为其他地址；
- DNS 方法：HiPER 向指定的 DNS 服务器发送 DNS 检测包，以检测线路是否激活。此方法中，检测目标只能为某 DNS 服务器的地址，不能为网关地址。

各方法支持的检测目标类型及使用限制如表 4-4 所示，其中，“网关”指对应线路的下一跳网关，“其他”指除网关之外的其他检测目标。“检测目标 IP 地址”用来设置欲检测的其他目标的 IP 地址。

检测方法	检测目标类型	检测目标 IP 地址	说明
ICMP	网关	无需设置	ICMP 可检测网关和其他目标
	其他	需设置	
ARP	网关	无需设置	PPPoE 上网时，不可使用该方法
DNS	其他	需设置	检测目标只能是 DNS 服务器

表 4-4 各种检测方法支持的检测地址类型

在实际应用中，选择检测方法时，供参考的依据及注意事项如下：

1. ICMP 方法检测线路灵敏度、准确度高，建议优先选用 ICMP 检测。
2. ARP 方法只能检测接入线路的下一跳网关，当需要检测其他目标地址（比如某 DNS 服务器）时，只能选择 ICMP 或 DNS 检测。PPPoE 上网时，不提供 ARP 方法。
3. DNS 方法，检测目标必须是 DNS 服务器，建议使用当地运营商提供的 DNS 服务器。注意，不能选择局域网内部主机使用的 DNS 服务器作为检测目标，否则，这些主机只能使用对应的线路上网，无法使用另外那条线路。
4. 部分线路不转发 ICMP 包（禁 ping），此时需选择 ARP 或 DNS 检测方法。

5. PPPoE 上网，系统提供的缺省配置是不启用线路检测，PPPoE 会使用自身的检测机制来检测线路。PPPoE 上网时，PPPoE 还可以增加 ICMP、DNS 的检测方式，但不能用来检测网关。

4.2.1.4　相关的静态路由

当配置了主线路、备份线路后，系统会自动生成相应的缺省路由，可在 ***WEB 管理界面—>系统状态—>路由和端口信息—>路由表信息列表***（章节 7.5.1）查看到对应路由信息，即“目的地址”为“0.0.0.0/0”的路由。如果主线路（备份线路）为静态 IP 或动态 IP 上网方式时，还可在 ***WEB 管理界面—>高级配置—>路由配置—>路由信息列表***（章节 6.4.4）中查看它们，具体描述请参考章节 6.4.2 中的表 6-17。

当主线路（备份线路）使用线路检测后，系统还会自动生成相应的静态路由，用来限制检测目标地址时由指定的端口（或线路）外出。可在 ***WEB 管理界面—>高级配置—>路由配置—>路由信息列表***（章节 6.4.4）中查看它们，即“路由 ID”为“Detect”（对应主线路）、“DetectDMZ”（对应备份线路）的静态路由。注意，静态 IP 或动态 IP 上网方式时，且检测“网关”时，无需使用这两条路由，将直接使用线路的缺省路由检测线路。

4.2.2 线路组合配置

4.2.2.1　线路备份

图 4-14 线路组合配置——线路备份

- 线路检测方法：检测线路是否激活的方法，选项为“ICMP”、“ARP”及“DNS”。
  ICMP：使用向网关或预先指定的其他检测目标发送 ICMP 包的方式检测线路是否激活；

ARP：使用向网关发送 ARP 包的方式检测线路是否激活。

DNS：使用向预先指定的某 DNS 服务器发送 DNS 包的方式检测线路是否激活；

- 线路组合方式：线路的组合方式，选项为“ 线路备份 ”或“ 负载均衡 ”，这里选中“ 线路备份 ”；
- 检测目标类型：欲检测的目标的类型，选项为“ 网关 ”、“ 其他 ”。ARP 方式下，仅支持检测“ 网关 ”；DNS 方式下，仅支持检测“ 其他 ”；ICMP 方式下，两个都支持。

网关：线路的检测目标为该线路下一跳网关；

其他：线路的检测目标为用户自定义的其他检测目标；

- 检测间隔：发送检测包的时间间隔，单位：毫秒。启用线路检测时，取值范围为 1000～60000 毫秒。该值为 0 时，表示不启用线路检测；
- 检测次数：检测周期内发送检测包的次数（每次发送一个检测包）。缺省值：3 次；
- 检测目标 IP 地址：欲检测的目标的 IP 地址。当“ 检测目标类型 ”为“ 其他 ”时，需配置该参数；“ 检测目标类型 ”为“ 网关 ”时，无需配置该参数；
- 优先级：主线路（或备份线路）连接成功后，该线路的路由优先级，值越低优先级越高。目的网段相同的情况下，HiPER 将优先选择优先级高的线路转发数据包；
- 断开优先级：主线路（或备份线路）断开后，该线路的路由优先级，值越低断开优先级越高。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 为保证双线路连接和工作正常，线路的优先级应高于断开优先级，同时，主线路的优先级、断开优先级必须分别高于备份线路的优先级、断开优先级；

2. 线路备份实现机制如下所述：当主线路正常时，由于主线路比备份线路的优先级高，因此 HiPER 将选择主线路转发数据包；若主线路出现故障，由于其断开优先级比备份线路的优先级低，因此 HiPER 将选择备份线路转发数据包；一旦主线路恢复正常，它又重新使用线路连接后的优先级，相应地，HiPER 会选择主线路转发数据包。

4.2.2.2　负载均衡

负载均衡方式下，HiPER 可实现以下功能：

1)　根据目的 IP 地址指定线路

HiPER 允许用户预先为到某个特定的目的地址或网段的路由指定线路，它是通过配置调度规则（静态路由）来实现的。某些情况下，运营商之间相互访问对方的服务器速度很慢；这时，可以通过配置调度规则，为到固定目的地址或网段的路由指定线路，以保证正常使用网络服务器。

如果配置了调度规则，那么所有对其设置的目的地址或网段的访问都必须使用其绑定线路。当该调度规则绑定的线路有故障时，将无法访问该目的地址。

2)　根据源 IP 地址指定优先线路

HiPER 允许用户预先为局域网中的某些主机指定上网线路，它是通过设置线路的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”来实现的，IP 地址属于两个地址范围内的主机将优先使用指定线路。对于已指定上网线路的主机来说，当指定线路正常时，它们只能通过该线路上网；但是，当指定线路有故障时，它们会使用另外一条线路上网。

3)　根据线路带宽合理地分配流量

HiPER 允许用户预先指定分配到两条线路的流量的比例，它是通过设置线路的“ 权重 ”来实现的。

在实际应用中，当局域网中的主机均未指定上网线路时，可根据两条线路的带宽比来设置各线路的“ 权重 ”，从而实现按带宽来分配流量。例如，如果主线路和备份线路的带宽分别为 6M、4M，则可将主线路、备份线路的“ 权重 ”分别设 3、2，分配到主线路、备份线路的流量比将接近 3:2。

而当局域网中的某些主机指定了上网线路时，若按照带宽比来设置线路的“ 权重 ”，分配到两条线路的流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整“ 权重 ”。

4)　提供两种流量分配规则

“ 分配规则 ”用来控制线路流量，它作用于局域网中没有指定上网线路的计算机，HiPER 提供两种分配规则：“ NAT 会话 ”和“ IP 地址 ”，它们的实现机制如下所述。

a)　IP 地址

使用 IP 地址作为分配规则时，HiPER 将根据线路的“ 权重 ”，把未指定上网线路主机的 IP 地址，按顺序依次分配到两条线路。分配到两条线路的 IP 地址的数量比为线路的“ 权重 ”比，来自同一 IP 地址的 NAT 会话使用同一条线路。

例如，若主线路和备份线路的“ 权重 ” 分别为 3、2，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用主线路，第 4、5 台主机将使用备份线路，第 6、7、8 台主机将使用主线路，第 9、10 台主机将使用备份线路，……，依此类推。注意，这里假设每台主机均只有一个 IP 地址。

b)　NAT 会话

使用 NAT 会话作为分配规则时，HiPER 将根据线路的“ 权重 ”，把未指定上网线路的主机发起的 NAT 会话，将按顺序依次分配到两条线路。分配到两条线路的 NAT 会话的数量比为线路的“ 权重 ”比，同一主机发起的 NAT 会话可使用两条线路。

例如，若主线路和备份线路的“ 权重 ” 分别为 3、2，则根据连接的先后顺序，局域网内主机发起的第 1、2、3 个 NAT 会话将使用主线路，第 4、5 个 NAT 会话将使用备份线路，接着第 6、7、8 个 NAT 会话将使用主线路，第 9、10 个 NAT 会话将使用主线路，……，依此类推。

一般情况下，建议“ 分配规则 ”选择为“ IP 地址 ”。当对带宽要求高，需要双线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择“ NAT 会话 ”，从而能够充分利用双线路带宽，以提高下载速度。需要注意的是，即便选择了“ NAT 会话 ”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

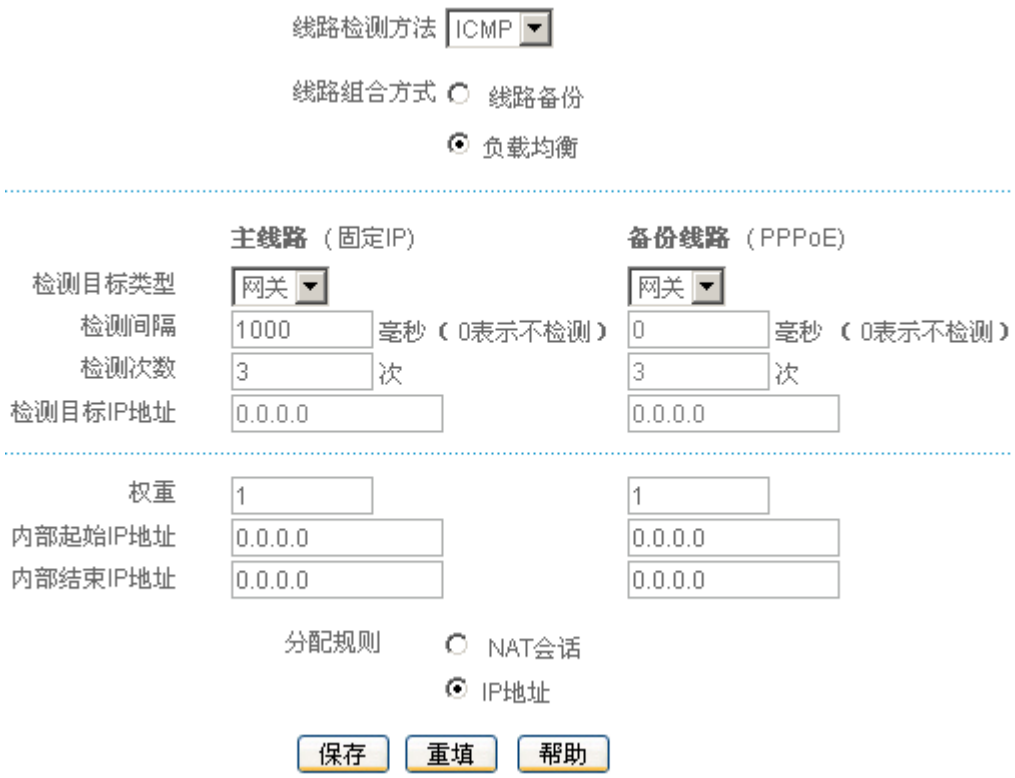


图 4-15 线路组合配置——负载均衡

“ 负载均衡 ”方式下，“ 线路检测方法 ”、“ 检测目标类型 ”、“ 检测间隔 ”、“ 检测次数 ”、“ 检测目标 IP 地址 ”这几个参数的涵义，与“ 线路备份 ”方式下相关参数涵义相同，请参考相关参数描述。

- 线路组合方式：线路的组合方式，选项为“ 线路备份 ”或“ 负载均衡 ”，这里选中“ 负载均衡 ”；
- 权重：主线路（备份线路）的权重，取值范围为 1-255（取整数），缺省值为 1；
- 内部起始 IP 地址、内部结束 IP 地址：局域网内优先使用指定线路（主线路或备份线路）上网的计算机的起始 IP 地址和结束 IP 地址；
- 分配规则：控制线路流量时使用的规则。选项为“ NAT 会话 ”或“ IP 地址 ”，缺省值为“ IP 地址 ”。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：对于高级用户来说，可以到 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 规则***（章节 6.3.3）中配置、修改本页面相关参数。

4.2.2.3　配置线路组合

第一步，进入 ***WEB 管理界面—>基本配置—>线路组合***页面；

第二步，如有需要，选择“ 线路检测方法 ”，选择主线路和备份线路的“ 检测目标类型 ”，并根据实际要求有选择地设置“ 检测间隔 ”、“ 检测次数 ”及“ 检测目标 IP 地址 ”。

第三步，选择“ 线路组合方式 ”：“ 线路备份 ”或“ 负载均衡 ”；

第四步，分为两种情况：

若选择“ 线路备份 ”作为线路组合方式，则分别填入主线路和备份线路的“ 优先级 ”、

“ 断开优先级 ”；

若选择“ 负载均衡 ”作为线路组合方式，则分别填入主线路和备份线路的“ 权重 ”，并选择“ 分配规则 ”，如有需要，再分别填入两条线路的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”；

第五步，单击“ 保存 ”按钮，线路组合配置完成。

4.2.2.4　线路组合配置实例

1.　应用需求

某网吧使用双线路上网，主线路为固定 IP 接入，带宽为 6M；备份线路为 PPPoE 拨号上网，带宽为 4M，希望采取负载均衡的方式上网，同时指定游戏区的计算机（IP 地址范围：192.168.16.10～192.168.16.60）通过主线路上网，指定普通区的计算机（IP 地址范围：192.168.16.110～192.168.16.140）通过备份线路上网，网吧内的其余计算机不受限制。

主线路和备份线路检测均采用系统缺省配置，主线路检测相关配置：“ 检测方法 ”为“ ICMP ”，“ 检测地址类型 ”为“ 网关 ”、“ 检测间隔 ”为“ 1000 毫秒 ”，“ 检测次数 ”为“ 3 次 ”。备份线路为 PPPoE 上网，缺省情况下不启用线路检测，相关配置：“ 检测目标类型 ”为“ 网关 ”，“ 检测间隔 ”为“ 0 毫秒 ”。

2.　分析

由于主线路和备份线路的带宽分别为 6M 和 4M，因此可以将主线路的“ 权重 ”设为 3，备份线路的“ 权重 ”设为 2；“ 分配规则 ”选用“ IP 地址 ”。

3.　配置步骤

第一步，进入 ***WEB 管理界面—>基本配置—>线路组合***页面；

第二步，选择“ 线路组合方式 ”为“ 负载均衡 ”，如图 4-16 所示；

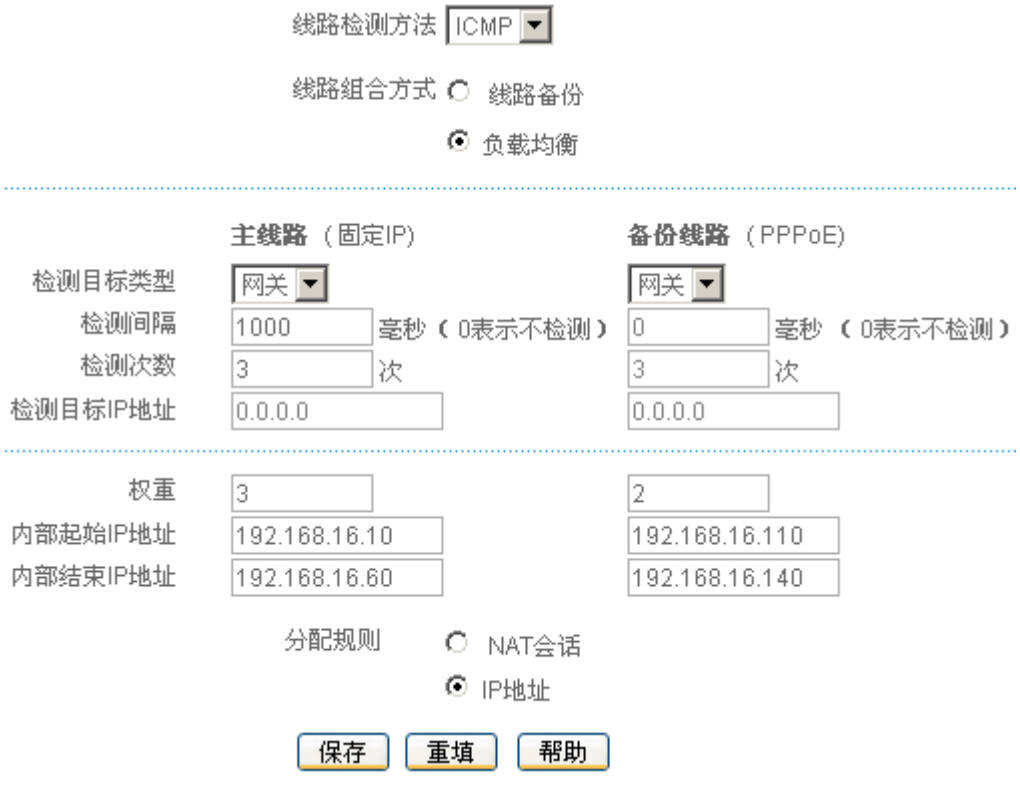


图 4-16　线路组合配置——实例

第三步，在主线路的“ 权重 ”中填入 3，在备份线路的“ 权重 ”中填入 2，

第四步，在主线路的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.10、192.168.16.60；在备份线路的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.110、192.168.16.140；

第五步，选择“ 分配规则 ”为“ IP 地址 ”；

第六步，单击“ 保存 ”按钮，线路组合配置完成。

配置完成后，可以在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 规则***（章节 6.3.3）中的“ NAT 规则信息列表 ”中查看到相关信息。

4.2.3 查看双线路状态

双线路组合配置成功之后，可以在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中查看双线路相关信息。

另外，在 ***WEB 管理界面—>系统状态—>路由和端口信息—>路由表信息列表***（章节 7.5.1）中可以看到两条线路的路由信息：

1. 负载均衡时的缺省路由信息（以两条固定 IP 接入为例），如表 4-5 所示，此时局域网中的计算机按照线路组合相关配置，分别从两条线路 61.12.150.21（ie2—DMZ/WAN2 口线路）和 200.200.200.254（ie1—WAN 口线路）实现上网。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第　页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	61.12.150.21	ie2	lugpamNF	60	1	0	17
0.0.0.0/0	200.200.200.254	ie1	lugpamNF	60	1	0	127

表 4-5 路由表信息列表——实例一

2. 负载均衡时的一条线路中断时的缺省路由信息（以两条固定 IP 接入为例），如表 4-6 所示，中断的线路路由状态前有标记“ * ”，此时局域网所有计算机从 200.200.200.254（ie1—WAN 口线路）实现上网。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第　页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	8
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	120	1	0	45

表 4-6 路由表信息列表——实例二

3. 线路备份时的缺省路由信息（以两条固定 IP 接入为例），如表 4-7 所示，备份线路的路由状态前有标记“ * ”，此时局域网所有计算机从 200.200.200.254（ie1—WAN 口线路）实现上网。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第　页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	20
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	61	1	0	20

表 4-7 路由表信息列表——实例三

4.2.4 调度规则配置

配置调度规则即快速配置静态路由，一条调度规则对应一条静态路由。某些情况下，运营商之间相互访问对方的服务器速度很慢，运营商可能还会禁止别的运营商访问自己的服务器；这时，可以通过配置调度规则，为到固定目的地址或网段的路由指定出口线路，以保证正常使用网络服务器。

4.2.4.1 调度规则配置

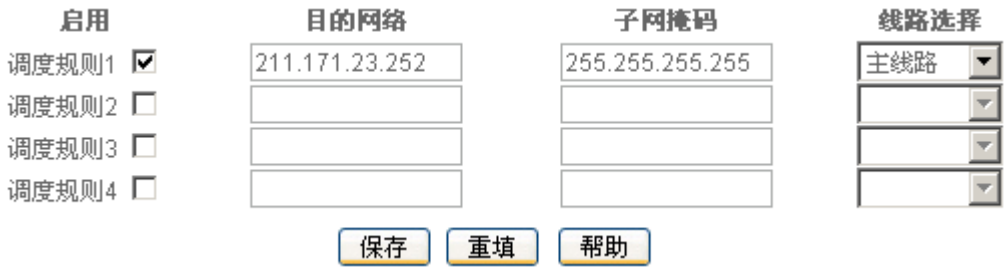


图 4-17 调度规则配置

- 启用：启用或者是取消调度规则 1～调度规则 4，选中是启用；
- 目的网络：该调度规则的目的网络号；
- 子网掩码：该调度规则的目的网络的掩码；
- 线路选择：该调度规则所绑定的线路。
  主线路：绑定的线路为主线路；
  备份线路：绑定的线路为备份线路。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 调度规则配置完成后，可以在 ***WEB 管理界面—>高级配置—>路由配置***（章节 6.4）中的“ 路由信息列表 ”查看到相关信息，即“ 路由 ID ”为“ sysDD1～sysDD4 ”的静态路由，它们可以编辑修改，但不能删除；
2. 如果调度规则所绑定的线路被删除（***WEB 管理界面—>基本配置—>ISP 配置*** 〈章节 4.1.2〉），该调度规则也被删除。

4.2.4.2 自定义调度规则

第一步，进入 ***WEB 管理界面—>基本配置—>线路组合—>调度规则配置***页面；
第二步，选中某一条调度规则；
第三步，输入该调度规则指向的“ 目的网络 ”及“ 子网掩码 ”；
第四步，选择“ 线路选择 ”为“ 主线路 ”或“ 备份线路 ”；
第五步，单击“ 保存 ”按钮，该调度规则配置完成。

提示：若要删除某条已配置的调度规则，只需单击该调度规则后的方框（方框变为空），再单击“ 保存 ”按钮，该规则即被删除。

4.2.4.3　调度规则配置实例

例如，用户通过双线路上网，主线路是电信的线路；备份线路是网通的线路。电信上有某个服务器（IP 地址：211.171.23.252），如果用户通过网通的线路连接它，速度将非常慢。这时我们就可以将到该服务器的路由绑定到主线路上，以提高上网速度，具体配置如图 4-17 所示。配置完成后，可以在 ***WEB 管理界面—>高级配置—>路由配置***（章节 6.4）中的“ 路由信息列表 ”查看到相关信息。

4.3　DHCP 和 DNS 服务器

本节主要讲述 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***的配置方法。

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、DNS 服务器以及一些扩展信息等。为局域网中的所有计算机正确的配置 TCP/IP 协议是一件非常繁琐的事情。HiPER 能够配置成 DHCP 服务器，为局域网计算机动态分配 IP 地址、子网掩码、网关、以及 DNS 服务器、WINS 服务器等信息。

4.3.1 DHCP 服务配置

图 4-18 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或允许 HiPER 的 DHCP 服务器功能。选中为允许，如图 4-18 所示；
- 起始 IP 地址：DHCP 服务器给局域网计算机自动分配的起始 IP 地址（一般要和 HiPER 的局域网端口 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给局域网计算机自动分配的子网掩码（一般要和 HiPER 局域网的端口子网掩码一致）；
- 总地址数：DHCP 服务器可以分配的地址总数量；
- 网关 IP 地址：DHCP 服务器给局域网计算机自动分配的网关 IP 地址（一般要和 HiPER 的局域网端口 IP 地址一致）；
- 租用时间：局域网计算机获得 HiPER 分配的 IP 地址的租用时间（单位：秒）；
- 主 DNS 服务器：DHCP 服务器给局域网计算机自动分配的主用 DNS 服务器的 IP 地址，此处会自动识别在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）或者在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）中主线路设置的值；

- 备 DNS 服务器：DHCP 服务器给局域网计算机自动分配的备用 DNS 服务器的 IP 地址，此处会自动识别在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）或者在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）中主线路设置的值；
- 启用 DNS 代理：选中之后，HiPER 会启用 DNS 代理功能，此时给局域网中的计算机分配的主 DNS 服务器的 IP 地址就是 HiPER 局域网端口的 IP 地址。
- 主 WINS 服务器：DHCP 服务器给局域网计算机自动分配的主用 WINS 服务器的 IP 地址，没有可以不填；
- 备 WINS 服务器：DHCP 服务器给局域网计算机自动分配的备用 WINS 服务器的 IP 地址，没有可以不填；
- 保存：DHCP 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 启用了 DNS 代理功能之后，必须要设置一个 ISP（例如中国电信）提供的可用的主 DNS 服务器；
2. 如果要使用 HiPER 的 DHCP 服务器功能，局域网计算机的 TCP/IP 协议必须设置为“ 自动获得 IP 地址 ”；
3. 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS Server 设置为代理服务器的 IP 地址，那么，只需将 HiPER 的局域网 IP 地址设置为同一个 IP 地址，这样，当 HiPER 启用 DNS 代理功能之后，用户不需要修改计算机的配置就可以转换到使用 HiPER。

4.3.2 DHCP 地址池使用信息

表 4-8 DHCP 地址池使用信息

- 显示 DHCP 地址池使用信息：选中后，系统将显示“ DHCP 地址池使用信息列表 ”，如表 4-8 所示；
- ID：地址使用者的序号；
- IP 地址：DHCP 服务器分配的 IP 地址；
- MAC 地址：使用该 IP 地址的网络设备的 MAC 地址。“ ?????pending????? ”表示该 IP 地址在租期时间范围内，但该网络设备已经离线，如果在租期内该网络设备再次申请 IP 地址，仍将获得该 IP 地址；

- 掩码：DHCP 服务器分配的 IP 地址的子网掩码；
- 剩余租期：租用该 IP 地址的剩余时间（时间单位：天:时:分:秒）；
- 刷新：如果想查看最新的 DHCP 池地址使用信息，单击右下角的“ 刷新 ”按钮，将显示最新的 DHCP 地址池使用信息。

4.3.3 配置 DHCP 服务器

第一步，进入 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 启用 DHCP 服务器 ”选项，根据需要填写“ 起始 IP 地址 ”、“ 子网掩码 ”、“ 总地址数 ”、“ 网关地址 ”、“ 租用时间 ”、“ 主 DNS 服务器 ”、“ 备份 DNS 服务器 ”等信息；

第三步，如果希望启用 HiPER 的 DNS 代理功能，则需要选中“ 启用 DNS 代理 ”选项，此时局域网中计算机分配到的 DNS 服务器是 HiPER 局域网端口的 IP 地址；

第四步，根据需要选择是否填写“ 主 WINS 服务器 ”，“ 备 WINS 服务器 ”；

第五步，单击“ 保存 ”按钮，DHCP 服务器配置生效。

提示：如果要关闭 DHCP 服务器功能，请取消“ 启用 DHCP 服务器 ”的选中，单击“ 保存 ”按钮。

4.3.4 DHCP 手工绑定配置

使用 DHCP 服务为局域网中的计算机自动配置 TCP/IP 属性是非常方便的，但是会造成一台计算机不同时间被分配到不同 IP 地址的现象。而某些局域网计算机可能需要固定的 IP 地址，这时就需要使用 DHCP 手工绑定功能，将计算机的 MAC 地址与某个 IP 地址绑定，如图 4-19 所示。当具有此 MAC 地址的计算机向 DHCP 服务器（HiPER）申请地址时，HiPER 将根据其 MAC 地址寻找到对应的固定 IP 地址分配给该计算机。

图 4-19 DHCP 手工绑定配置

- IP 地址：预留的 IP 地址，必须是 DHCP 服务器指定的地址范围内的合法 IP 地址；
- MAC 地址：固定使用该预留 IP 地址的计算机的 MAC 地址；
- 用户名：欲配置该 DHCP 手工绑定的计算机的用户名（自定义，不能重复）。取值范围：1～31 个字符。
- 保存：DHCP 手工绑定配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：设置成功后，HiPER 将为指定计算机固定分配预设的 IP 地址。

4.3.5 DHCP 手工绑定列表

表 4-9 DHCP 手工绑定列表

- 增加 DHCP 手工绑定：选中“ 添加 ”选项，如图 4-19 所示，输入 DHCP 手工绑定信息，单击“ 保存 ”按钮，生成新的 DHCP 手工绑定；
- 浏览 DHCP 手工绑定：如果已经生成了 DHCP 手工绑定，只需选中“ 显示 DHCP 手工绑定信息 ”，即可浏览“ DHCP 手工绑定信息列表 ”，如表 4-9 所示；
- 编辑 DHCP 手工绑定：如果想编辑某一 DHCP 手工绑定，只需单击此条 DHCP 手工绑定后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除 DHCP 手工绑定：选中一些 DHCP 手工绑定信息条目，单击右下角的“ 删除 ”按钮，即可删除那些被选中的 DHCP 手工绑定。

4.3.6 自定义 DHCP 手工绑定

第一步，进入 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 添加 ”选项，填写“ 用户名 ”、“ MAC 地址 ”和预设的“ IP 地址 ”；

第三步，单击“ 保存 ”按钮，然后可以在“ DHCP 手工绑定信息列表 ”中看到添加的记录；

第四步，继续添加新的 DHCP 手工绑定用户。

提示：删除 DHCP 手工绑定，选中“ 显示 DHCP 手工绑定信息 ”选项，在“ DHCP 手工绑定信息列表 ”中选中要删除的 DHCP 手工绑定信息条目，单击“ 删除 ”按钮。

4.4　端口配置

本节主要讲述 ***WEB 管理界面—>基本配置—>端口配置***的配置方法。

4.4.1 端口配置

在本页面，可以修改 HiPER 的物理端口的 IP 地址、MAC 地址及工作模式，并且可以给各个端口配置第二个 IP 地址，实现多网络互相连接，如图 4-20 所示。

图 4-20 端口配置

- IP 地址 1：该端口的 IP 地址；
- 子网掩码 1：该端口的子网掩码；
- IP 地址 2：该端口的第二个 IP 地址；
- 子网掩码 2：该端口的第二子网掩码；
- MAC 地址：该端口的 MAC 地址（一般情况下不需要修改）；
- 模式 :该端口的工作模式。Auto—自适应，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
- 保存：端口配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. HiPER 支持为每个物理路由端口配置两个不同网段的 IP 地址，支持连接两个不同的网段，而且可以相互通讯；
2. 如果改变了 LAN 端口的“ IP 地址 ”，在保存之后，必须使用新的 IP 地址才能登录 WEB 界面管理，并且，局域网中计算机的默认网关必须设置成该 IP 地址才能正常上网；
3. 可以到 ***WEB 管理界面—>系统状态—>路由和端口信息***（章节 7.5）中查看端口实际连接状态。

4.4.2 配置 IP 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置 IP 地址的物理端口；

第三步，设置该端口的 IP 地址和子网掩码：在“ IP 地址 1 ”中填入 IP 地址，在“ 子网掩码 ”中填入子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：在这里可以快速配置、修改各端口的 IP 地址和子网掩码。

4.4.3 配置第二个 IP 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置第二个 IP 地址的物理端口；

第三步，设置该端口的第二个 IP 地址和子网掩码：在“ IP 地址 2 ”中填入第二个 IP 地址，在“ 子网掩码 2 ”中填入第二个子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置第二个 IP 地址。只有在同一个端口需要配置两个不同网段的情况下，才配置第二个 IP 地址。

4.4.4 配置 MAC 地址

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置 MAC 地址的物理端口；

第三步，设置该端口的 MAC 地址：在“ MAC 地址 ”中填入该端口的 MAC 地址；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置 MAC 地址。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备的 MAC 地址设置成和原有网络设备的 MAC 地址相同。

4.4.5 配置以太网工作模式

第一步，进入 ***WEB 管理界面—>基本配置—>端口配置***页面；

第二步，选择需要配置以太网工作模式的物理端口；

第三步，设置该端口的工作模式：在“ 模式 ”中选择工作模式。

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要修改，即端口默认自适应工作模式。如有兼容性问题，或使用的设备不支持自动协商功能，才需要设置该端口的工作模式。

4.5　DDNS 配置

本节主要讲述 ***WEB 管理界面—>基本配置—>DDNS 配置***的配置方法。

提示：只有在***系统管理—>时钟管理—>系统时间设置***（章节 5.2）中正确配置了 HiPER 的系统时间和时区信息，DDNS 功能才能正常工作。

动态域名解析服务（DDNS）是将一个固定的域名解析成动态变化的 IP 地址（如 ADSL 拨号上网）的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务的收取一定的费用。在此情况下，艾泰科技会尽可能及时通知。如拒绝支付该等费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

目前，艾泰科技仅提供对 iplink.com.cn 的 DDNS 服务的支持，将来还将陆续提供对其他 DDNS 服务的支持。

4.5.1 申请 DDNS 帐号

请登录 http://reg.iplink.com.cn 申请后缀为 iplink.com.cn 的二级域名。

动态域名注册表

（ IPLINK.COM.CN ）

公司名称:	上海艾泰科技有限公司
地址:	上海市世纪大道1500号东方大厦1429室
邮编:	200122
电话:	021-50623736
传真:	021-68416675
联系人:	艾泰科技
电子邮件:	support@utt.com.cn
管理员用户名:	support
管理员密码:	********
确认密码:	********
主机名:	utt .iplink.com.cn
动态域名用途:	☐ 网站 ☑ VPN ☐ VoIP ☐ 其它
注册类型:	○ 付费 ○ 购买产品 产品名称: HiPER路由器 序 列 号: 4201183
注：为更好的提供服务，请填写所有栏目，否则注册无效。 我们不会把注册信息在未经您授权的情况下用于其它任何场合。 提示：将鼠标停留在每个项目上可以查看相应的填写说明。	
提交　重填	

表 4-10 动态域名注册表

- 主机名：填入欲申请的二级域名（为避免重复，请填写 HiPER 底板上的全球唯一序列号 S/N）；
- 序列号：产品序列号。它和 HiPER 的 ***WEB 管理界面—>基本配置—>DDNS 配置—>配置 DDNS 服务***（章节 4.5.2）中的“ 注册号 ”必须一致。
- 提交：单击“ 提交 ”按钮，即可获得 HiPER 匹配该二级域名的 ENKEY（请妥善保管此密码）；

enKey: T94eOJBlYOK+5gNNP9seYXUMeXvAWpVJtlbVRvNsdID6

- 重填：重新填写动态域名注册表。
- 提示：同一个域名只能被注册一次，而且在使用不同的 HiPER 申请同一个域名时获得的“ enkey ”是不同的，所以在更换 HiPER 而没有更换域名时，需要登录 http://reg.iplink.com.cn 的管理界面先删除原先申请的域名，之后再重新申请。

4.5.2 配置 DDNS 服务

图 4-21 DDNS 服务配置

- 启用 DDNS 服务：启用或者禁用 DDNS 服务，选中为启用，如图 4-21 所示；
- 注册域名：点击 http://reg.iplink.com.cn 超连接，即可进入该页面申请域名；
- 注册号：产品注册号。
- 服务商：选择提供域名服务的服务商，目前只支持 iplink.com.cn 的 DDNS 服务；
- 主机名：申请 DDNS 帐号时使用的主机名。为避免重复，请使用 HiPER 的底板上的全球唯一序列号 S/N 申请；
- 域名：选择指定 DDNS 服务商提供的域名；
- 密码：申请 DDNS 帐号时得到的 ENKEY；
- 确认密码：申请 DDNS 帐号时得到的 ENKEY，此处与上栏所填密码一致；
- 保存：DDNS 配置生效；
- 重填：恢复到修改前的配置参数。

4.5.3 DDNS 状态

图 4-22 DDNS 状态

- 更新状态：单击“ 更新状态 ”按钮，可将当前 PPPoE 连接的 IP 地址更新到动态域名系统中。

常用 DDNS 状态信息解释如表 4-11 所示。

状态信息	信息涵义
Tot: 1, Succ: 1, Fail:0	共更新 1 次，成功 1 次，失败 0 次
Last update: Thu Jun 10 09:53:41 2004	最后更新时间为 2004 年 6 月 09:53:41
Ip: 61.171.212.7	当前分配的 IP 地址
Hostname: utt.iplink.com.cn	主机名（动态域名）
ddns update result : Success	将当前 PPPoE 连接的 IP 地址（61.171.212.7）成功更新到动态域名（utt.iplink.com.cn）上

表 4-11 DDNS 状态信息

4.5.4 DDNS 验证

可以在局域网计算机的 DOS 状态下，使用 Ping 命令（例如：ping utt.iplink.com.cn）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：61.171.212.7），证明域名解析正确。注意：一般情况下，HiPER 在使用 NAT 后，从 Internet 上将不能 ping 通 HiPER 的 IP 地址，只能解析出该域名对应的 IP 地址。

```
C:\>ping utt.iplink.com.cn

Pinging utt.iplink.com.cn [61.171.212.7] with 32 bytes of data:
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255

Ping statistics for 61.171.212.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

提示：

1. DDNS 功能目前只支持主线路（接在 WAN 口的线路）是 PPPoE 的情况，而且必须先通过 WEB 管理界面配置了 PPPoE 连接才能正常工作。没有配置或者是通过其他方式配置 PPPoE 连接，系统会弹出如图 4-23 所示对话框：

图 4-23 对话框——请先配置 PPPoE

2. ISP（例如中国电信）分配给主线路（接在 WAN 口的线路）的 PPPoE 连接线路的 IP 地址是公网 IP 地址的时候才能保证该域名能被 Internet 的用户访问；

3. 不同 HiPER 注册相同的域名得到的 ENKEY 不同；
4. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射；
5. 出现如下错误信息，如图 4-24 所示，请检查：在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 5.2）中检查当前系统时钟是否正确；在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.6.3）中检查 PPPoE 连接是否成功；在 http://reg.iplink.com.cn 检查在线申请的 ENKEY 是否正确。

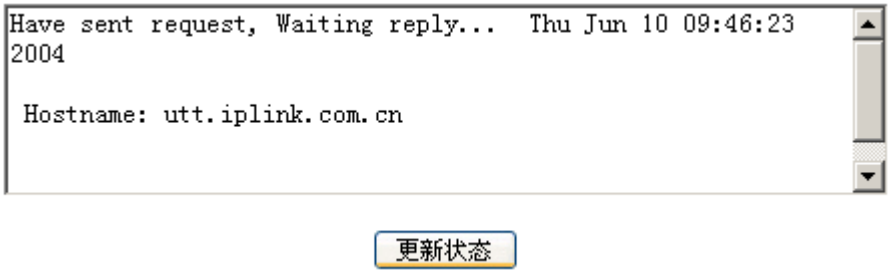


图 4-24 DDNS 状态

6. 暂停 DDNS 更新服务：在 ***WEB 管理界面—>基本配置—>DDNS 配置—>配置 DDNS 服务***（章节 4.5.2）页面，取消“启用 DDNS 服务”的选中，单击“保存”按钮即可暂停 IP 地址的更新。但是，如果你暂停了 DDNS 服务，而且 WAN 口已经离线并且释放了 IP 地址。当这个被释放的 IP 地址被 ISP 分配给其他用户使用时，此时解析域名仍旧会解析到这个 IP 地址，这样就有可能造成域名和实际用户不符的现象。

4.6　时间段配置

本节主要讲述 ***WEB 管理界面—>基本配置—>时间段配置***的配置方法。

提示：只有在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 5.2）中，为 HiPER 设置了正确的时间后，时间段功能才能正常工作。

配置时间段策略，可以被某些高级功能（如拨号时间段、业务管理）引用，以控制这些业务的生效时间，从而达到控制上网费用、控制游戏时间等目的。

一个时间段最多可以由 8 个时间单元组成，同时还可通过参数“开始日期和时间”和“结束日期和时间”设置该时间段的生效时间（如图 4-25）。当时间段有效期已过，该时间段无效。“开始日期和时间”、“结束日期和时间”均设成 1990 年 1 月 1 日 00:00:00，代表该时间段永久有效。

4.6.1 时间段配置

图 4-25 时间段配置

- 时间段名称：时间段策略的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 开始日期和时间：该时间段策略生效的开始日期和时间，系统默认为 1989 年 1 月 1 日 00:00:00（单位：时:分:秒）；
- 结束日期和时间：该时间段策略失效的结束日期和时间，系统默认为 2010 年 1 月 1 日 00:00:00（单位：时:分:秒）；

- 时间段一~时间段八：该时间段要控制的时间单元，一个时间段最多可由 8 个时间单元组成；
- 类型：时间单元的类型，类型有每天、星期一、星期二、……、星期日、工作日（周一至周五）、周末（周六、周日）等；
- 开始时间：每个时间单元的开始时间，系统默认为 00:00:00（单位：时:分:秒）；
- 结束时间：每个时间单元的结束时间，系统默认为 23:59:59（单位：时:分:秒）；
- 保存：时间段配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：一个跨越零点的连续时间段，必须配置成两个连续的时间单元，例如，从晚上 8 点到次日凌晨 5 点需要以 24:00:00 分为两个时间段，即第一个时间单元为 20:00:00~23:59:59，第二个时间单元为 00:00:00~5:00:00。

4.6.2 时间段列表

表 4-12 时间段信息列表

- 增加时间段：选中“ 添加 ”选项，输入时间段信息，单击“ 保存 ”按钮，生成新的时间段；
- 浏览时间段：如果已经配置了时间段，可在“ 时间段信息列表 ”中浏览相关信息，如表 4-12 所示；
- 编辑时间段：如果想编辑某一时间段，只需单击此时间段条目中的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除时间段：选中一些时间段，单击右下角的“ 删除 ”按钮，即可删除被选中的时间段；
- 查看时间段详细信息：单击某个时间段条目中的“ 详细 ” 超链接，可显示该时间段的详细信息，以及被其他功能（如业务管理）引用的相关信息，如图 4-26 所示。

图 4-26 时间段详细信息

4.6.3 自定义时间段

第一步，进入 ***WEB 管理界面—>基本配置—>时间段配置***页面；

第二步，单击“ 添加 ”按钮，填写时间段名称；

第三步，根据需要填写该时间段的起止时间；

第四步，填写时间段具体时间单元信息；

第五步，单击“ 保存 ”按钮，时间段配置完成，可在“ 时间段信息列表 ”中看到添加的记录；

第六步，继续添加新的时间段信息。

提示：

1. 若要删除时间段，只需在“ 时间段信息列表 ”中选中要删除的时间段，单击“ 删除 ”按钮，即可删除；

2. 某一时间段正在被某些高级功能（如 PPPoE 拨号、业务管理）引用时，不可删除。

4.6.4 时间段配置实例

1. 应用需求

2004 年度某公司为控制销售部门员工的上网行为，针对其实际需求，规定在工作时间中只允许 WEB 业务，在其余时间则开放所有业务。该公司的工作时间为：周一~周五，上午 9 点~12 点，下午 1 点~6 点；中午 12 点~13 点为午间休息时间。

2. 分析

由上，可以将该公司上网时间划分为工作时间（worktime）和休息时间（freetime）两个时间段。

1) 工作时间段划分为 2 个时间单元，具体信息如下：

开始日期和时间：2004 年 1 月 1 日 00:00:00

结束日期和时间：2004 年 12 月 31 日 23:59:59
时间段一：类型为“ 工作日（周一至周五）”，开始时间 09:00:00，结束时间 11:59:59
时间段二：类型为“ 工作日（周一至周五）”，开始时间 13:00:00，结束时间 17:59:59

2)　由于休息时间段划分为 4 个时间单元，具体信息如下：
开始日期和时间：2004 年 1 月 1 日 00:00:00
结束日期和时间：2004 年 12 月 31 日 23:59:59
时间段一：类型为“ 工作日（周一至周五）”，开始时间 00:00:00，结束时间 08:59:59
时间段二：类型为“ 工作日（周一至周五）”，开始时间 12:00:00，结束时间 12:59:59
时间段三：类型为“ 工作日（周一至周五）”，开始时间 18:00:00，结束时间 23:59:59
时间段四：类型为“ 周末（周六、周日）”，开始时间 00:00:00，结束时间 23:59:59

3.　配置步骤

第一步，进入 ***WEB 管理界面—>基本配置—>时间段配置***页面；

第二步，配置工作时间段“ worktime ”。选中“ 添加 ”选项，如图 4-25 所示，在“ 时间段名称 ”中填入 worktime；

第三步，设置 worktime 起止时间：
在“ 开始日期和时间 ”中填入 2004 年 1 月 1 日 00:00:00，
在“ 结束日期和时间 ”中填入 2004 年 12 月 31 日 23:59:59；

第四步，分别设置该时间段的 2 个时间单元，首先选择类型，然后填入开始时间和结束时间：
时间段一：在“ 类型 ”中选择“ 工作日（周一至周五）”，
在“ 开始时间 ”中填入 09:00:00，在“ 结束时间 ”中填入 11:59:59；
时间段二：在“ 类型 ”中选择“ 工作日（周一至周五）”，
在“ 开始时间 ”中填入 13:00:00，在“ 结束时间 ”中填入 17:59:59；
第五步，单击“ 保存 ”按钮，时间段 worktime 设置成功；

第六步，配置休息时间段“ freetime ”。选中“ 添加 ”选项，如图 4-27 所示，在“ 时间段名称 ”中填入 freetime；

图 4-27 时间段配置——实例

第七步，设置 freetime 起止时间：

在“开始日期和时间”中填入 2004 年 1 月 1 日 00:00:00，

在“结束日期和时间”中填入 2004 年 12 月 31 日 23:59:59；

第八步，分别设置该时间段的 4 个工作单元，首先选择类型，然后填入开始时间和结束时间。

时间段一：在“类型”中选择“工作日（周一~周五）”，

在“开始时间”中填入 00:00:00，在“结束时间”中填入 08:59:59；

时间段二：在“类型”中选择“工作日（周一~周五）”，

在“开始时间”中填入 12:00:00，在“结束时间”中填入 12:59:59；

时间段三：在“类型”中选择“工作日（周一~周五）”，

在“开始时间”中填入 18:00:00，在“结束时间”中填入 23:59:59；

时间段四：在“类型”中选择“周末（周六、周日）”，

在“开始时间”中填入 00:00:00，在“结束时间”中填入 23:59:59；

第九步，单击“保存”按钮，时间段 freetime 设置成功。

至此，时间段配置成功，在“时间段信息列表”（如表 4-12）中，可以查看和编辑时间段“worktime”和时间段“freetime”的具体信息。

第5章　系统管理

在系统管理中，主要设置 HiPER 相关管理参数，包括管理员配置、时钟管理、软件升级、配置管理、WEB 服务器配置、SNMP 配置、SYSLOG 配置等等。

5.1　管理员配置

本节主要讲述 ***WEB 管理界面—>系统管理—>管理员配置***的配置方法，如图 5-1 所示。

5.1.1 WEB 界面管理员配置

图 5-1 管理员配置

- 管理员用户名：新 WEB 管理员的用户名。自定义，不能重复。取值范围：1～31 个字符；
- 密码：该管理员的登录密码；
- 确认密码：该管理员的登录密码，此处必须和上一栏所填密码一致；
- 管理员组：该管理员所属的管理员组，不同的管理员组提供不同级别的管理权限，同一个组中的管理员具有相同的管理权限。系统提供“ 浏览 ”、“ 执行 ”及“ 系统管理 ”三个管理员组，各组提供的权限如下：
  浏览：只能查看相关页面的配置。***WEB 管理界面—>上网监控***（章节 8）页面除外；
  执行：可以查看并且修改相关页面的配置。不能修改 ***WEB 管理界面—>系统管理—>管理员配置***（章节 5.1）页面，不能查看或修改 ***WEB 管理界面—>上网监控***（章节 8）页面；
  系统管理：可以任意查看和修改相关页面的配置；
- 允许 telnet 远程登录：允许或者禁止该管理员通过 telnet 管理 HiPER，选中为允许。只有“ 系统管理 ”组中的管理员才有 telnet 权限，而且最多只允许设置 3 个有 telnet 权限的管理员。
- 保存：管理员配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. HiPER 允许用户使用同一个“ 管理员用户名 ”从多个 IP 地址同时登录。注意，为

避免配置冲突，建议同时只从一个 IP 地址登录修改配置；

2. 为安全起见，强烈建议修改初始的管理员密码，并谨慎保管管理员用户名及密码。

5.1.2 管理员信息列表

表 5-1 管理员信息列表

- 增加管理员：选中“ 添加 ”选项，输入管理员信息，单击“ 保存 ”按钮，生成新的管理员；
- 浏览管理员：如果已配置了管理员，可在“ 管理员信息列表 ”中浏览相关信息，如表 5-1 所示；
- 编辑管理员：如果想编辑某一管理员，只需单击该管理员条目后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除管理员：选中一些管理员，单击右下角的“ 删除 ”按钮，即可删除被选中的管理员。

提示：系统默认管理员 Default 不能删除或者编辑名称。

5.2 时钟管理

本节主要讲述 ***WEB 管理界面—>系统管理—>时钟管理***的配置，如图 5-2 所示。

为了保证 HiPER 各种涉及到时间的功能（如 DDNS 服务、时间段配置等）正常工作，需要准确地设定 HiPER 的时钟，使其与当地标准时间同步。

HiPER 支持“ 手工设置时间 ”或者“ 网络时间同步 ”两种方式来设置系统时间，但是每次只能选择其中的一种方式来设置时间。

部分型号的产品没有时间保存功能，HiPER 重启后时间会恢复到出厂值，请使用“ 网络时间同步 ”功能来从互联网上获取标准的时间，当下次开机连接到 Internet 后，HiPER 将会自动获得标准的时间。

图 5-2 时钟管理配置

- 当前系统时间：显示当前 HiPER 时钟（单位：年:月:日，时:分:秒）；
- 时区选择：选择 HiPER 所在地的国际时区，只有选择了正确的时区，网络时间同步（sntp）功能才能正常工作；
- 手工设置时间：手工输入当前的日期和时间（单位：年:月:日，时:分:秒）；
- 网络时间同步（sntp）：使用网络时间同步功能，设置了正确的 sntp 服务器后，当 HiPER 连接到 Internet 之后，就会自动和所设置 sntp 服务器同步时间。系统缺省预设两个 sntp 服务器 192.43.244.18、129.6.15.28，一般情况下不需要修改，若需更多 sntp 知识及服务器，请访问 http://www.ntp.org。
- 保存：时钟管理配置参数生效；
- 重填：恢复到修改前的配置参数。

5.3　软件升级

本节主要讲述 ***WEB 管理界面—>系统管理—>软件升级***的配置方法。

5.3.1 显示和保存当前运行软件

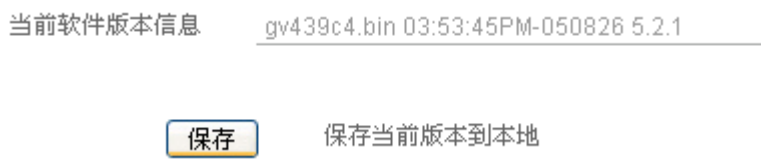
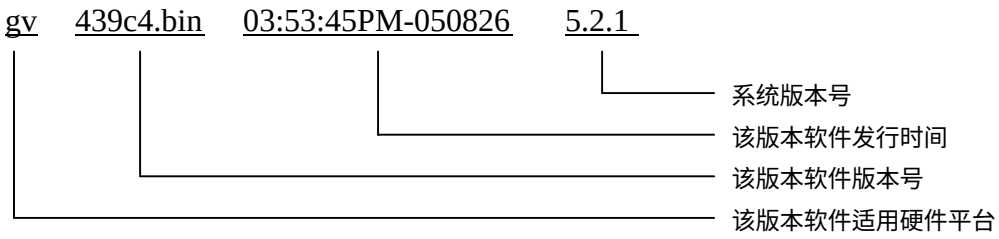


图 5-3 显示和保存当前软件

版本信息含义如下：



保存：将系统当前运行的软件备份到管理计算机的硬盘中。

提示：在这里只保存系统的运行软件，并没有保存系统当前的配置文件。

5.3.2 软件升级

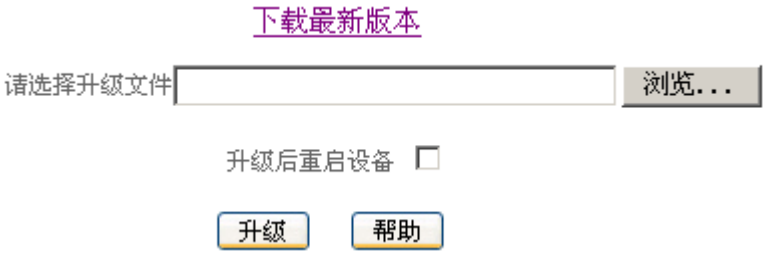


图 5-4 软件升级

第一步 下载最新软件

单击“ 下载最新版本 ”超链接，到艾泰科技官方网站下载最新的软件版本到本地计算机。

提示：

1. 请选择合适型号的最新软件；下载的软件适用的硬件平台必须和当前产品的硬件平台一致，软件版本必须比当前使用的软件版本新；
2. 建议升级之前，先到 ***WEB 管理界面—>系统管理—>配置管理***（章节 5.4）备份系统当前配置。

第二步 选择升级软件所在路径

在“请选择升级文件”文本框中输入将要升级的软件在本地计算机的路径，或者是通过“浏览”在本地计算机选择新软件。

- 升级后重启设备：升级软件成功之后，必须重启 HiPER，新软件才能生效。可以选择“升级后重启设备”，HiPER 将在软件升级成功后自动重启。如果不选择“升级后重启设备”，请在升级成功后选择合适的时间重启 HiPER。

第三步 更新 HiPER 的软件

单击“升级”按钮，更新 HiPER 的软件。

提示：

1. 强烈建议在 HiPER 负载比较轻（用户比较少）的情况下升级；
2. 定期的升级 HiPER 的软件，可以使 HiPER 获得更多的功能或者更佳的工作性能。正确的软件升级并不会改变当前 HiPER 设置；
3. 升级过程不能关闭 HiPER 电源，否则将会导致不可预期的错误甚至不可恢复的硬件损坏；
4. 如果升级失败，可以到 ***WEB 管理界面—>系统状态—>系统异常信息***（章节 7.7）中检查失败信息。

5.4　配置管理

本节主要讲述 ***WEB 管理界面—>系统管理—>配置管理***的配置方法。

5.4.1 保存当前配置

图 5-5 保存配置

- 保存：将 HiPER 当前运行的配置下载到管理员计算机中，并保存成一个文本文件。

5.4.2 恢复备份配置

图 5-6 恢复备份配置

- 加载：在“ 请选择配置文件 ”文本框中输入将要恢复的配置在本地计算机的路径和名称，或者是通过“ 浏览 ”在本地计算机选择配置文件，单击“ 加载 ”按钮，将备份的配置文件恢复到 HiPER 中。

提示：HiPER 在恢复配置前会自动清空当前配置，恢复到出厂配置。

5.4.3 恢复出厂配置

图 5-7 恢复出厂配置

- 恢复：将 HiPER 的配置恢复到出厂时的设置值。

提示：

1. 这是一个非常危险的操作，它将删除所有自定义的配置，并将系统恢复到原始状态。强烈建议在恢复出厂配置之前，在 ***WEB 管理界面—>系统管理—>配置管理—>保存当前配置***（章节 5.4.1）中，将 HiPER 运行的配置保存；
2. HiPER 的出厂用户名为：Default；默认密码为空；默认 LAN 口 IP 地址/子网掩码为：192.168.16.1/ 255.255.255.0；
3. 将 HiPER 的配置恢复到出厂值以后，建议在 ***WEB 管理界面—>系统管理—>配置管理—>重新启动设备***（章节 5.4.4）中，重启 HiPER。

5.4.4 重新启动设备

图 5-8 重新启动设备

- 重启：将 HiPER 重新启动一次。
- 提示：重启时，所有的用户将断开到 HiPER 的连接，请谨慎使用此功能。

5.5 WEB 服务器

本节主要讲述 ***WEB 管理界面—>系统管理—>WEB 服务器***的配置方法，如图 5-9 所示。在本页面，主要配置 HiPER 的 WEB 管理界面后台服务器的相关参数。

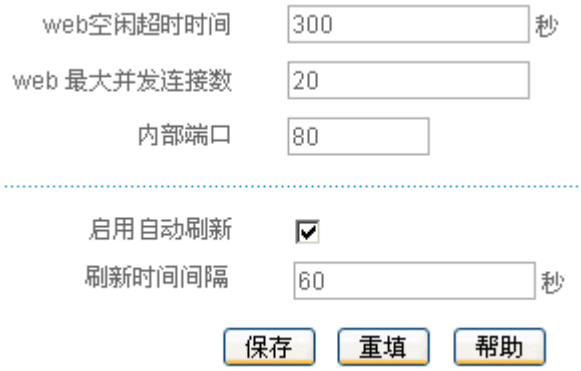


图 5-9 WEB 服务器配置

- web 空闲超时时间：通过 WEB 管理界面管理 HiPER 时，如果超过该时间没有任何操作，HiPER 的 Web Server 将自动断开与浏览器的连接。缺省值为 300 秒；
- web 最大并发连接数：管理员通过 WEB 配置 HiPER 时，将会有多条 TCP 连接连到 HiPER。该参数默认值是 20，建议不要减小该值。如果访问 WEB 管理界面时出现页面显示不完整的情况，可适当增大该值。但该值超过 100 时，将可能降低 HiPER 抗 TCP SYN FLOOD 病毒攻击的能力。
- 内部端口：从局域网通过 WEB 管理 HiPER 的 HTTP 端口，默认为 80。如果修改该参数，就必须用“IP 地址：端口”的方式（例如 http://192.168.16.1:88）才能登录 HiPER。
- 启用自动刷新：启用或者关闭自动刷新功能。启用自动刷新功能后，HiPER 的 Web Server 将每隔单位时间自动刷新当前页面（根据页面状态决定是否刷新）；
- 刷新时间间隔：HiPER 的 Web Server 自动刷新 WEB 界面的间隔时间（单位：秒）。
- 保存：WEB 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：为保障 HiPER 有足够的性能提供服务，请尽可能减少 Web 并发连接的数量，同时不要选择自动刷新。

5.6　SNMP 配置

本节主要讲述 ***WEB 管理界面—>系统管理—>SNMP 配置***的配置方法，如图 5-10 所示。

SNMP 是一系列协议组和规范，它提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。在 HiPER 上启用了 SNMP 服务，就可以在远程使用 SNMP 软件管理和监视 HiPER。

图 5-10 SNMP 配置

- 启用 SNMP 服务：禁止或者允许 SNMP 服务。为安全起见，目前只允许 SNMP 服务器读 HiPER 信息，不允许 SNMP 服务器修改 HiPER 信息；
- SNMP 社区名：配置 SNMP 社区名，它必须和 SNMP 网络管理软件包配置匹配；
- 只允许以下主机管理：选中“只允许以下主机管理”后，可以设置 1~3 台主机，只有这三台主机可以通过 SNMP 管理 HiPER；
- 允许主机 1，2，3：可通过 SNMP 管理 HiPER 的主机的 IP 地址。
- 保存：SNMP 配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：必须在 ***WEB 管理界面—>系统管理—>远程管理***（章节 5.8）中允许了从 Internet 通过 SNMP 管理 HiPER，才能从 Internet 通过 SNMP 服务器远程管理 HiPER。

5.7　SYSLOG 配置

本节主要讲述 ***WEB 管理界面—>系统管理—>SYSLOG 配置***（如图 5-11）的配置方法。

syslog 里面记载了 HiPER 的大量运行信息，是管理员每日需要查看的记录。对管理员分析系统的状况、监视 HiPER 的活动来说，是一个相当重要的部分。

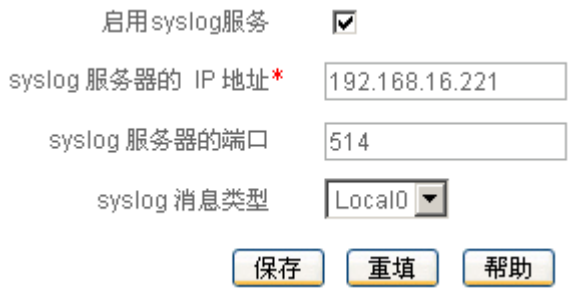


图 5-11 SYSLOG 配置

- 启用 syslog 服务：启用或禁用 syslog 服务，选中为启用；
- syslog 服务器的 IP 地址：远程 syslog 服务器的 IP 地址；
- syslog 服务器的端口：远程 syslog 服务器所开放的服务端口，一般默认为 514；
- syslog 消息类型：local0~local7，由 syslog 管理员自定义的一些消息类型。
- 保存：syslog 配置参数生效；
- 重填：恢复到修改前的配置参数。

5.8　远程管理

本节主要讲述 ***WEB 管理界面—>系统管理—>远程管理***的配置方法。

由于 HiPER 内置了防火墙，将会屏蔽所有来自 Internet 的连接。如果要从 Internet 远程管理 HiPER，首先必须开启“ 允许 Internet 远程管理 ”，然后再启用相关的远程管理功能。但是如果关闭了 NAT 功能，相关功能将失效。

图 5-12 远程管理

- 允许 Internet 远程管理：开启或者关闭远程管理功能，选中为开启；
- HTTP：允许或禁止从 Internet 通过 WEB 管理 HiPER，HiPER 默认外部 WEB 管理端口为 8081 。如要从 Internet 通过 WEB 管理 HiPER 必须用“ IP 地址：端口 ”的方式（例如 http://218.21.31.3:8081）才能登录 HiPER；
- 外部端口：可以修改 HiPER 默认外部端口（默认值为 8081）。注意，这个端口修改成 80 以后，在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射配置***中，就会增加一条 TCP80 端口的映射，此时如需要再次增加局域网 WEB 服务器的映射，就会引起冲突。
- SNMP：允许或禁止从 Internet 通过 SNMP 管理 HiPER，选中为允许；
- TELNET：允许或禁止从 Internet 通过 TELNET 管理 HiPER，选中为允许。
- 保存：远程管理配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. HiPER 的 Internet 地址可以从 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中获得；
2. 为安全起见，如非必要，请不要打开允许 Internet 远程管理功能；
3. 开启 Internet 远程管理功能之前，请先到 ***WEB 管理界面—>系统管理—>管理员配置***（章节 5.1）中修改 HiPER 默认密码；
4. 如果上网线路采用了 PPPoE 拨号，其 IP 地址是动态的，可以在 ***WEB 管理界面—>基本配置—>DDNS 配置***（章节 4.5）中配置 DDNS 功能；
5. 打开了 HTTP、SNMP、TELNET 管理功能之后，系统会自动生成 TCP:8081 端口、UDP:161 端口、TCP:23 端口的 NAT 映射（可在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射列表***〈章节 6.3.4.2〉中查看），它们均绑定在主线路上；
6. 当在 ***WEB 管理界面—>快速向导—>上网接入线路配置***〈章节 3.2.4〉或 ***WEB 管理界面—>基本配置—>ISP 配置***〈章节 4.2.2〉中，删除了主线路或改变其上网接入方式之后，本页面相关配置也将被删除，需要重新配置所需的远程管理功能；
7. 在寻求艾泰科技工程师服务之前，请事先打开相关远程管理功能。

第6章　高级配置

本章主要讲述如何设置 HiPER 的组管理、IP 业务管理、NAT 和 DMZ 配置、静态路由、用户管理、特殊功能等高级属性的相关参数。

6.1　组管理

本节主要讲述 ***WEB 管理界面—>高级配置—>组管理***的配置方法。

在 HiPER 引入了工作组这个概念，可以将具有共同性质（如业务要求相同）的用户划分在同一个工作组中，并给他们分配连续的 IP 地址，如图 6-1 所示。HiPER 允许配置只有一个用户的特殊工作组，其开始 IP 地址和结束 IP 地址相同，我们将之称为个人用户。

不同工作组的 IP 地址不能重叠；但是个人用户的 IP 地址可以与其它某工作组中的某个 IP 地址相同，即允许创建属于某工作组的个人用户。

配置了工作组之后，就可在 ***WEB 管理界面—>高级配置—>业务管理***（章节 6.2）中为工作组中的用户定义上网权限和时间，在 ***WEB 管理界面—>带宽业务***（章节 9）中为工作组中的用户定义上网下行带宽。

如果某个工作组在业务管理（***WEB 管理界面—>高级配置—>业务管理***〈章节 6.2〉）或带宽业务（***WEB 管理界面—>带宽业务***〈章节 9〉）中被引用的话，编辑该组起始地址和结束地址，相关业务的引用同时发生改变；并且，该组将不能删除，这时候，必须首先取消相关引用，才能删除。

6.1.1 工作组配置

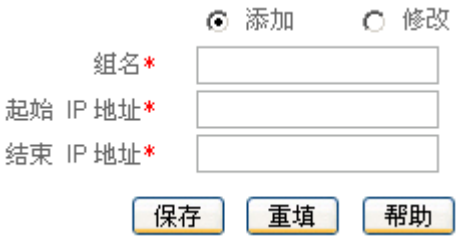


图 6-1 工作组配置

- 组名：工作组的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 起始 IP 地址：该工作组的起始 IP 地址；
- 结束 IP 地址：该工作组的结束 IP 地址。
- 保存：工作组配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：HiPER 支持内建多个工作组，其中 IPSSG 组为系统默认工作组，其起止地址均为 0.0.0.0。IPSSG 组包括局域网中未配置业务策略的所有用户，该工作组不能编辑和删除。

6.1.2 工作组列表

表 6-1 组信息列表

- 增加工作组：选中“ 添加 ”选项，输入工作组信息，单击“ 保存 ”按钮，生成新的工作组；
- 浏览工作组：如果已经生成了工作组，可在“ 组信息列表 ”中浏览相关信息，如表 6-1 所示；
- 编辑工作组：如果想编辑某一工作组，只需单击此工作组后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除工作组：选中一些工作组，单击右下角的“ 删除 ”按钮，即可删除被选中的工作组。

提示：如果在 ***WEB 管理界面—>高级配置—>业务管理***（章节 6.2）中定义了新个人用户策略，在“ 组信息列表 ”将自动增加该用户的信息记录，即增加只有一个用户的特殊工作组，其“ 组名 ”为该用户的 IP 地址；同时，只能在此处才能删除该特殊工作组。

6.1.3 自定义工作组

第一步，规划局域网中的 IP 地址，将局域网 IP 划分成若干个连续的地址段，注意将具有共同性质的用户放在一个组里，实现统一管理。例如一个部门可以分为一个组。

第二步，进入 ***WEB 管理界面—>高级配置—>组管理***页面；

第三步，选择“ 添加 ”选项，输入工作组的“ 组名 ”、“ 起始 IP 地址 ”和“ 结束 IP 地址 ”，然后单击“ 保存 ”按钮；

第四步，该工作组添加成功后，可以在“ 组信息列表 ”中看到相应的记录；

第五步，继续配置其他工作组。

提示：删除工作组，在“ 组信息列表 ”中选中要删除的工作组，单击“ 删除 ”按钮，即可删除被选中的工作组。

6.1.4 工作组配置实例

1. 应用要求

某公司为实现上网统一管理，针对各部门上网实际需求，决定对管理部门、技术部门、销售部门进行分组管理，将这三个部门划分成三个工作组，从而能够实现对这三个部门的上网行为控制。各工作组具体配置信息如表 6-2 所示：

部门名	组名	起始 IP 地址	结束 IP 地址
销售部门	Sale	192.168.16.50/24	192.168.16.70/24
技术部门	Technique	192.168.16.120/24	192.168.16.150/24
管理部门	Admin	192.168.16.160/24	192.168.16.180/24

表 6-2 工作组配置信息

2. 配置步骤

第一步，规划局域网中的 IP 地址，如表 6-2 所示；

第二步，进入 ***WEB 管理界面—>高级配置—>组管理***页面；

第三步，配置工作组 Sale。选择“ 添加 ”选项，如图 6-2 所示。在“ 组名 ”中填入“ Sale ”，在 “ 起始 IP 地址 ” 中填入 “ 192.168.16.50 ”，在 “ 结束 IP 地址 ” 中填入 “ 192.168.16.70 ”，然后单击 “ 保存 ” 按钮，工作组 Sale 配置完成。

图 6-2 工作组 Sale 配置

第四步，配置工作组 Technique。选择 “ 添加 ” 选项，如图 6-3 所示。在 “ 组名 ” 中填入 “ Technique ”，在 “ 起始 IP 地址 ” 中填入 “ 192.168.16.120 ”，在 “ 结束 IP 地址 ” 中填入 “ 192.168.16.150 ”，然后单击 “ 保存 ” 按钮，工作组 Technique 配置完成。

图 6-3 工作组 Technique 配置

第五步，配置工作组 Admin。选择 “ 添加 ” 选项，如图 6-4 所示。在 “ 组名 ” 中填入 “ Admin ”，在 “ 起始 IP 地址 ” 中填入 “ 192.168.16.160 ”，在 “ 结束 IP 地址 ” 中填入 “ 192.168.16.180 ”，然后单击 “ 保存 ” 按钮，工作组 Admin 配置完成。

图 6-4 工作组 Admin 配置

至此，三个工作组均配置完成，可以在 “ 组信息列表 ” 中查看这三个工作组的相关信息，如表 6-1 所示。

6.2　业务管理

本节主要讲述 ***WEB 管理界面—>高级配置—>业务管理***的配置方法。

本页面由“ 业务策略配置 ”和“ 业务策略信息列表 ”两大部分组成，用户自定义的业务策略将按配置顺序或预先指定的位置排列在“ 业务策略信息列表 ”中。

提示：需要先在 ***WEB 管理界面—>高级配置—>组管理***（章节 6.1）中定义工作组，才能在本页面为工作组用户定义上网业务策略；需要先在 ***WEB 管理界面—>基本配置—>时间段配置***（章节 4.6）中定义时间段，才能在本页面定义业务策略的有效时间。

6.2.1 业务管理功能介绍

HiPER 默认合法的 IP 地址将被允许连接和通过 HiPER，但是可在本页面定义若干业务策略，从而控制局域网用户的上网行为，比如限制用户不能访问某些网站，或者只能访问某些网站，限制用户访问一些服务（如只需访问 WWW 和电子邮件服务，其他服务如 TELNET 则禁止），或只允许一些主机访问网络等等。灵活地运用 HiPER 的业务管理功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户在不同时段的 Internet 访问权限。

启用了业务管理功能之后，HiPER 通过检查所有进入和外出的请求，确保局域网用户遵守这些业务策略。WEB UI 中，HiPER 默认检查来自局域网内部，从 LAN 口进入 HiPER 的数据包。

业务策略的过滤条件包括：源地址、目的端口、目的 IP 地址、源端口、协议、时间计划等。定义了这些过滤条件以后，就可以利用它们创建业务策略，并指定各条业务策略的动作（允许或禁止），从而对进入 HiPER 的数据包进行控制：转发或丢弃。

6.2.1.1　工作组、个人用户及 IPSSG 组

通过设置“ 组选择 ”可以指定业务策略要过滤的数据包的源地址，HiPER 提供三种类型的源地址对象：工作组，个人用户以及 IPSSG 组。HiPER 中，将这三种类型的策略分别成为工作组策略、个人用户策略及 IPSSG 组策略。

1.　工作组

一般情况下，业务策略是针对工作组定义的，该工作组的地址范围即为该策略要过滤数据包的源地址。同一个工作组的用户的上网权限完全相同，从而，你只需为工作组定义业务策略，而无需为每个用户分别定义业务策略。这样的话，不仅方便管理，也可以提高 HiPER 的工作效率。当然，你必须首先将上网要求相同的局域网用户定义在同一个工作组中，才能够为他们制定出正确而有效的业务策略。

当为某工作组配置了业务策略后，系统会自动生成该组的全局策略，默认是禁止该组除定义过的其他业务。工作组全局策略的名称为“ grpx_other ”，x 为阿拉伯数字，按照配置顺序依次为 1、2、3……。

2.　个人用户

同时，HiPER 也允许针对个人用户定义业务策略，该个人用户的 IP 地址即为该策略要

过滤的数据包的源地址。如果某个工作组中有个别用户的上网需求与该组其他用户基本相同，但同时也有少数一个或几个特别需求；或是某个用户突然有了新的上网需求时，就需要对这个用户单独定义业务策略。

注意，如果配置了个人用户策略，且该个人用户属于某个已经配置了业务策略的工作组，则该工作组的全局策略也对该个人用户起作用。

3. IPSSG 组

系统还提供一个默认工作组：IPSSG 组，包括局域网中没有定义业务策略的所有用户。允许针对 IPSSG 组定义业务策略，但该组的起止 IP 地址（均为 0.0.0.0）不能修改。

注意，如果配置了个人用户策略，且该个人用户不属于任何已配置了业务策略的工作组，则 IPSSG 组策略也对该个人用户起作用。

6.2.1.2 业务策略的动作

业务策略的动作包括转发和丢弃，对应的“动作”分别为“允许”或“禁止”。当需要处理的数据包与已定义的某条业务策略相匹配时，如果该策略的“动作”是“允许”，那么 HiPER 将转发该数据包；如果该策略的“动作”是“禁止”，那么 HiPER 将丢弃该数据包。

6.2.1.3 业务策略的类型及排列顺序

<table>
<tr><th>顺序</th><th colspan="2">类型</th><th>名称</th><th>备注</th></tr>
<tr><td rowspan="8">从上至下</td><td rowspan="3" colspan="2">系统缺省策略</td><td>lan</td><td rowspan="3">始终位于最上方，而且，“lan”未在“业务策略信息列表”中显示，不可编辑删除。“dns”、“dhcp”只可编辑其“动作”，不可删除。</td></tr>
<tr><td>dns</td></tr>
<tr><td>dhcp</td></tr>
<tr><td colspan="2">个人用户策略</td><td>自定义</td><td>由用户自定义的个人策略，始终位于工作组策略之上。</td></tr>
<tr><td rowspan="2">工作组策略</td><td>自定义的工作组策略</td><td>自定义</td><td rowspan="2">“grpx_other”只允许修改其“动作”。工作组策略始终位于IPSSG组策略之上。</td></tr>
<tr><td>工作组全局策略</td><td>grpx_other</td></tr>
<tr><td rowspan="2">IPSSG组策略</td><td>自定义的IPSSG组策略</td><td>自定义</td><td rowspan="2">“pass”始终位于自定义的IPSSG组策略之下，而且，未在“业务策略信息列表”中显示，不可编辑删除。</td></tr>
<tr><td>IPSSG组全局策略</td><td>pass</td></tr>
<tr><td colspan="2">系统全局策略</td><td>generic</td><td>始终位于最下方，而且，未在“业务策略信息列表”中显示，不可编辑删除。</td></tr>
</table>

表 6-3 业务策略类别及排列顺序

如表 6-3 所示，在启用了业务管理之后，系统会形成七种业务策略：

1. 为使 HiPER 正常工作而自动生成的名称为“lan”、“dns”以及“dhcp”的系统缺省业务策略，它们分别用来允许访问 LAN 口、允许 DNS、DHCP 服务；
2. 自定义的个人用户策略，可能是禁止或允许该用户的某项上网业务；
3. 自定义的工作组策略，可能是禁止或者允许该组的某项上网业务；

4. 系统自动生成的某工作组的全局策略，默认是禁止该组除定义过的其他业务。当为某工作组定义业务策略后，系统会自动生成该组的全局策略，名称为“ grpx_other ”，x 为阿拉伯数字，按照配置顺序依次为 1、2、3……；
5. 自定义的系统默认（IPSSG）组策略，可能是禁止或者允许 IPSSG 组的某项上网业务，但是该组的源起止 IP 地址不能修改；
6. 系统自动生成的 IPSSG 组的全局策略，默认是允许 IPSSG 组除定义过的其他业务，该业务策略的名称为“ pass ”。可在 ***WEB 管理界面—>高级配置—>业务管理—>业务管理全局配置***（章节 6.2.3）中，通过设置“ 允许其它用户 ”来指定其“ 动作 ”，默认是选中，表示允许；
7. 系统自动生成的全局策略（作用于局域网所有用户），允许所有数据包（包括其他非 IP 类型的包）通过，该业务策略的名称为“ generic ”。

一般情况下，所有的业务策略将按照如表 6-3 中的顺序排列在“ 业务策略信息列表 ”中，其中，按照从上到下的顺序依次是：最上面为“ lan ”、“ dns ”及“ dhcp ”这 3 条策略，之后是自定义的个人用户策略，然后是工作组策略，最下面为“ pass ”和“ generic ”这 2 条策略。需要指出的是，“ lan ”、“ pass ”及“ generic ”这 3 条系统自动生成的策略未在“ 业务策略信息列表 ”中显示。

对于工作组策略来说，缺省情况下，工作组策略将按照配置时的顺序从上到下依次排列，自定义的工作组策略将自动位于该组全局策略上方，但用户可以通过参数“ 插入位置 ”指定或调整某工作组策略的位置，并且，只能是在某工作组内部或工作组之间调整。注意，如果将某条自定义的工作组策略插入到该工作组全局策略下方，这条策略将不再起作用。

对于个人用户策略来说，缺省情况下，个人用户策略将按照配置时的顺序从上到下依次排列，但用户可以通过参数“ 插入位置 ”指定或调整某个人用户策略的位置，并且，只能在个人用户策略之间调整。

6.2.1.4　业务策略的执行顺序

WEB UI 中默认是在 LAN 口启用业务管理功能，HiPER 将检查来自局域网内部，从 LAN 口进入 HiPER 的数据包。

当来自局域网内部的数据包到达 LAN 口后，HiPER 将从“ 业务策略信息列表 ”的顶端开始向下搜索该表，查找第一个与数据包的源地址、目的地址、协议、目的端口、源端口以及接收到数据包请求的时间相匹配的策略。匹配的第一个策略将被应用于数据包，将不再检查后面的策略。如果没有找到匹配的策略，出于安全考虑，该数据包将被丢弃。

由于 HiPER 将会对数据包执行第一个匹配的策略所定义的动作，因此，必须按照从特殊到一般的顺序安排、配置策略。特殊策略不排除位于列表下部的更一般性策略的应用，但位于特殊策略前的一般性策略会产生此排除效应。举个例子来说，要求禁止局域网某工作组用户使用 MSN 业务，允许其他所有业务，那么，禁止 MSN 业务的策略必须在允许所有业务的策略的上方。否则，如果允许所有业务的策略在上方，那么禁止 MSN 业务的策略将未起作用，该工作组用户将仍旧可以使用 MSN 业务。

6.2.2 业务策略配置

在这个页面，如图 6-5、6-6 所示，可以为工作组及个人用户配置各种上网业务的权限和时间。

图 6-5 业务策略配置

- 策略名：业务策略的名称。自定义，不能重复，取值范围为 1～11 个字符；
- 组选择：该业务策略控制的局域网用户，即源地址范围。提供三种类型的选项：自定义的工作组的“ 组名 ”,“ 新个人用户 ” 及 IPSSG。
  组名：为某工作组配置业务策略时，需选择该工作组的“ 组名 ”。选定工作组后，这一行的右边会显示该组用户的 IP 地址段；
  新个人用户：为局域网中的单个用户配置业务策略时，需选择“ 新个人用户 ”。定义时，需要在该行右边第一个下划线上输入该用户的 IP 地址；
  IPSSG：为系统默认组配置上网业务时，需选择“ IPSSG ”。该组作用于局域网中没有配置上网业务的所有用户，其起始 IP 地址和结束 IP 地址均不能修改；
- 协议 :该业务策略的协议类型 ;供选择的协议如下 :6（TCP）、17（UDP）、1（ICMP）、2（IGMP）、4（IPINIP）、47（GRE）、50（ESP）、51（AH）、89（OSPF）、9（IGRP）、46（RSVP）以及 0（所有）。其中，“ 0（所有）” 表示所有协议。
  附录 C 提供了常用协议号与协议名称的对照表；
- 常用服务提示：提供使用 TCP 协议和 UDP 协议的常用服务端口。其中，选项“ 所有 ” 表示所有端口：即 1～65535 端口。选择某端口号（服务）后，系统会自动添加“ 目的起始端口/目的结束端口 ”。
  附录 D 提供了常用服务端口与服务名对照表；
- 目的起始端口、目的结束端口：该业务策略的目的起始端口和结束端口，通过它们可以指定一段范围的目的端口。如果只定义一个目的端口，则将它们设置为同一个数值。取值范围均为 1～65535；
- 目的起始地址、目的结束地址：该业务策略的目的起始 IP 地址和结束地址，通过它们可以指定一段范围的目的 IP 地址。如果只定义一个目的 IP 地址，则将它们设置成同一个值；
- 源起始端口、源结束端口：该业务策略的源起始端口和结束端口，通过它们可以指定一段范围的源端口。如果只定义一个源端口，则将它们设置为同一个值。取值

范围均为 1～65535；

- 插入位置（之前）：该业务策略的插入位置，选项为已配置的业务策略的“ 策略名 ”，及 “ pass ”。“ pass ” 为 IPSSG 组的全局策略，具体涵义参见本章 6.2.1.3 节。
  策略名：选择某 “ 策略名 ” 后，该业务策略将插入到指定的业务策略之前；
  pass：选择 “ pass ” 后，该业务策略将插入到策略 “ pass ” 之前，作为 “ 业务策略信息列表 ” 中显示的最后一条策略；
- 动作：该业务策略的执行动作，选项为 “ 允许 ” 或 “ 禁止 ”。
  允许：允许与该业务策略匹配的数据包通过，即 HiPER 将转发该数据包；
  禁止：禁止与该业务策略匹配的数据包通过，即 HiPER 将丢弃该数据包；
- 时间段：该业务策略生效的时间，不设置为所有时间。如果配置之后需要删除，可以选择 “ 时间段 ” 下拉列表中的空选项。如果该时间段已经超过执行的起止生效时间，系统将认为此条策略没有时间限制。
- 保存：业务管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 在本页面配置了新个人用户业务策略后，在 ***WEB 管理界面—>高级配置—>组管理—>工作组列表***（章节 6.1.2）中将增加该用户的信息记录，其 “ 组名 ” 为该用户的 IP 地址。因此，在为该个人用户继续配置其他业务策略时，在 “ 组选择 ” 中只需直接选择该用户的 IP 地址即可；
2. 在本页面可以删除为该个人用户配置的业务策略，但无法删除其地址信息，这时需在 ***WEB 管理界面—>高级配置—>组管理—>工作组列表***（章节 6.1.2）中才可删除它；
3. 如果希望对某个人用户定义业务策略，也可以先在 ***WEB 管理界面—>高级配置—>组管理—>工作组列表***（章节 6.1.2）中配置该个人用户，然后在 “ 组选择 ” 中选择其 “ 组名 ”，即可为该用户配置业务策略。本页面 “ 组选择 ” 中提供的 “ 新个人用户 ” 相当于提供了一种配置个人用户策略的快捷方式。

6.2.3 业务管理全局配置

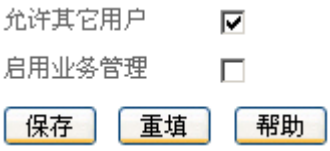


图 6-6 启用业务管理

- 允许其他用户：该参数对应 IPSSG 组的全局策略“ pass ”（具体涵义参见本章 6.2.1.3 节）的 “ 动作 ”，选中对应 “ 允许 ”，未选中对应 “ 禁止 ”。如果并没有为局域网里面的所有用户配置上网的业务策略，而又希望这些用户可以正常上网，那么就应该选中此项；
- 启用业务管理：启用或者关闭业务管理功能，选中为启用，使上面定义的业务策略开始工作。
- 保存：业务管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 当选择了 “ 允许其他用户 ” 之后，某些原来定义的没有上网业务权限的用户可能

会通过修改 IP 地址的方式来获得上网业务权限；

2. 在开启了“ 启用业务管理 ”之后，系统为工作正常，保留了一些业务策略，如 LAN、DNS 以及 DHCP 业务等作为内部使用。

6.2.4 业务策略信息列表

表 6-4 业务策略信息列表

业务策略信息列表
5/97
1/1 第一页 上一页 下一页 最后页 前往 第 页
源起始端口 源结束端口 目的起始端口 目的结束端口 目的起始地址 目的结束地址 时间段 编辑
0 0 53 53 0.0.0.0 0.0.0.0 编辑
0 0 67 67 0.0.0.0 0.0.0.0 编辑
1 65535 80 80 0.0.0.0 0.0.0.0 worktime 编辑
1 65535 21 21 0.0.0.0 0.0.0.0 freetime 编辑
0 0 0 0 0.0.0.0 0.0.0.0 编辑
全选 / 全不选
删除

表 6-5 业务策略信息列表（续表 6-4）

- 增加业务策略：选中“ 添加 ”选项，输入业务策略信息，单击“ 保存 ”按钮，生成新的业务策略；
- 浏览业务策略：如果已经生成了业务策略，可在“ 业务策略信息列表 ”（如表 6-4、6-5）中浏览相关信息；
- 编辑业务策略：如果想编辑某一业务策略，只需单击此业务策略的“ 策略名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除业务策略：选中一些业务策略，单击右下角的“ 删除 ”按钮，即可删除被选中的业务策略。

提示：“ 业务策略信息列表 ”中最上面的两条业务策略，即“ 策略名 ”为“ dns ”和“ dhcp ”的策略为系统缺省策略，它们可以编辑修改，但不能删除。

6.2.5 自定义业务策略

配置业务策略的过程如下：

第一步，进入 ***WEB 管理界面—>高级配置—>业务管理***页面；

第二步，选择“ 添加 ”选项，输入该策略的名称；

第三步，在“ 组选择 ”中选择该策略要匹配的工作组；或选择新个人用户，并填入该个人用户的 IP 地址；

第四步，根据欲配置的业务策略的要求有选择地填写“ 协议 ”、“ 目的起始端口 ”、“ 目的结束端口 ”、“ 目的起始地址 ”及“ 目的结束地址 ”，“ 源起始端口 ”、“ 源结束端口 ”；

第五步，如有需要，指定该业务策略的“ 插入位置 ”；

第六步，根据需要选择该业务的“ 动作 ”是“ 允许 ”或者“ 禁止 ”；

第七步，如有需要，在“ 时间段 ”中选择该业务策略的生效时间段；

第八步，单击“ 保存 ”按钮，生成新的业务管理策略；

第九步，该业务策略添加成功后，可以在“ 业务策略信息列表 ”中看到相应的记录；

第十步，在配置了工作组的业务策略后，系统会自动增加一条该工作组的全局策略，默认是禁止该组除定义过的其他业务，这条策略可以在“ 业务策略信息列表 ”中看到，“ 策略名 ”一般是 grpx_other（x 为阿拉伯数字）；

第十一步，继续配置其他业务策略；

第十二步，如果要禁止未配置上网业务策略的用户连接或者是通过 HiPER，可以取消“ 允许其他用户 ”的选中，否则的话，其他的用户将被全部允许；

第十三步，选中“ 启用业务管理 ”，然后单击“ 保存 ”按钮。

配置完成之后，所有受信的计算机连接和通过 HiPER 的数据包将会和“ 业务策略信息列表 ”中的策略比较，如果能够发现匹配的策略，HiPER 将按照该业务策略的“ 动作 ”来控制数据包：转发或丢弃。

6.2.6 业务策略配置实例

6.2.6.1 工作组策略配置实例

当配置了某工作组的业务策略后，系统会自动添加一个该工作组的全局策略，该策略的动作默认是禁止该工作组的所有业务，它结合该工作组已设置的其他业务策略形成该工作组完整的策略体系。在“ 业务策略信息列表 ”中，该工作组的全局策略将自动位于为该工作组自定义的业务策略的下方（可根据起止地址来判断该全局策略属于哪个工作组）。因此对于该工作组来说，当 HiPER 从网络接口上收到一个数据包时，将优先匹配该工作组自定义的业务策略，当这些业务策略均不匹配后，才去匹配该工作组的全局业务策略。

例如，当一个工作组设置一个允许 FTP 的策略，并且该工作组的全局策略的动作为禁止，那么，在“ 业务策略信息列表 ”中，FTP 策略将位于该组全局策略的上方。所有来自该组的 FTP 连接都将与这个 FTP 策略匹配，于是被允许通过。而其它任何类型服务的连接请求都将不会被这个 FTP 策略所匹配，于是，它们将去匹配该组全局策略，由于该组全局策略的动作为禁止，于是 HiPER 将禁止这条连接。

工作组的全局策略只允许编辑“ 动作 ”及“ 插入位置 ”。如果删除工作组的全局策略，IPSSG 组策略对该工作组用户也起作用。一般情况下，不要删除工作组的全局策略。

注意，可通过设置“ 插入位置 ”将某条自定义的工作组策略插入到该工作组全局策略下方，也可通过设置“ 插入位置 ”将某工作组全局策略移到该工作组某条自定义的业务策略的上方。上述任何一种情况下，对于某工作组来说，位于该工作组全局策略下方的自定义的业务策略将不再起作用。

下面将举例说明不同情况下，如何设置工作组的全局策略的动作。

需要说明的是：以下几个例子中的工作组“ Sale ”的具体配置可参见 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 6.1.4）。时间段“ worktime ”和“ freetime ”的具体配置可参见 ***WEB 管理界面—>基本配置—>时间段配置—>时间段配置实例***（章节 4.6.4）。

1. 如果要限制某一工作组只允许某些上网业务，那么该工作组的全局策略的动作应该设成禁止。

例如，要求：只允许“ Sale ”组的 WEB 业务，禁止该组其他所有上网业务。

要配置的策略是：

生成策略 1，允许“ Sale ”组的 WEB 业务；

系统会自动生成一条该组的全局策略 grp1_other，禁止该组用户的所有上网业务，如表 6-6、6-7 所示。

业务策略信息列表
4/97
1/1 第一页 上一页 下一页 最后页 前往 第 页
策略名 动作 协议 源起始地址 源结束地址 源起始端口 源结束端口 目的起始端口
dns 允许 17(UDP) 0.0.0.0 0.0.0.0 0 0 53
dhcp 允许 17(UDP) 0.0.0.0 0.0.0.0 0 0 67
1 允许 6(TCP) 192.168.16.50 192.168.16.70 1 65535 80
grp1_other 禁止 0(所有) 192.168.16.50 192.168.16.70 0 0 0
全选 / 全不选
删除

表 6-6 业务策略信息列表——实例一

业务策略信息列表
4/97
1/1 第一页 上一页 下一页 最后页 前往 第 页
源起始端口 源结束端口 目的起始端口 目的结束端口 目的起始地址 目的结束地址 时间段 编辑
0 0 53 53 0.0.0.0 0.0.0.0 编辑
0 0 67 68 0.0.0.0 0.0.0.0 编辑
1 65535 80 80 0.0.0.0 0.0.0.0 编辑
0 0 0 0 0.0.0.0 0.0.0.0 编辑
全选 / 全不选
删除

表 6-7 业务策略信息列表（续表 6-6）——实例一

2. 如果要限制某一工作组只禁止某些上网业务，那么该工作组的全局策略的动作应该设成允许。

例如，要求：只禁止“ Sale ”组的用户访问网站 http://www.playboy.com（IP 地址为

209.247.228.201）和网站 http://www.cnn.com（IP 地址为 64.236.24.12），允许该组其他所有上网业务。

要配置的策略是：

生成策略 1，禁止“ Sale ”组访问目的地址：209.247.228.201；

生成策略 2，禁止“ Sale ”组访问目的地址：64.236.24.12；

系统会自动生成一条该组的全局策略 grp1_other，这时需将其动作修改成“ 允许 ”，如表 6-8、6-9 所示。

业务策略信息列表　5/97

1/1　第一页　上一页　下一页　最后页　前往 第　页

策略名	动作	协议	源起始地址	源结束地址	源起始端口	源结束端口	目的起始端口
dns	允许	17(UDP)	0.0.0.0	0.0.0.0	0	0	53
dhcp	允许	17(UDP)	0.0.0.0	0.0.0.0	0	0	67
1	禁止	0(所有)	192.168.16.50	192.168.16.70	0	0	0
2	禁止	0(所有)	192.168.16.50	192.168.16.70	0	0	0
grp1_other	允许	0(所有)	192.168.16.50	192.168.16.70	0	0	0

全选 / 全不选　删除

表 6-8　业务策略信息列表——实例二

业务策略信息列表　5/97

1/1　第一页　上一页　下一页　最后页　前往 第　页

起始端口	源结束端口	目的起始端口	目的结束端口	目的起始地址	目的结束地址	时间段	编辑
0	0	53	53	0.0.0.0	0.0.0.0		编辑
0	0	67	68	0.0.0.0	0.0.0.0		编辑
0	0	0	0	209.247.228.201	209.247.228.201		编辑
0	0	0	0	64.236.24.12	64.236.24.12		编辑
0	0	0	0	0.0.0.0	0.0.0.0		编辑

全选 / 全不选　删除

表 6-9　业务策略信息列表（续表 6-8）——实例二

3.　如果要限制某一工作组的某些上网业务在不同时间段有不同的权限，那么该工作组的全局策略的动作应该设成禁止。

例如，要求：时间段“ worktime ”（工作时间）内只允许“ Sale ”组的 WEB 业务，时间段“ freetime ”（业余时间）开放 Sale 组的所有业务。

要配置的策略是：

生成策略 1，允许“ Sale ”组用户在时间段“ worktime ”的 WEB 业务；

生成策略 2，允许“ Sale ”组用户在时间段“ freetime ”的所有业务；

系统会自动生成一条该组的全局策略 grp1_other，禁止该组其他所有上网业务，如表 6-10、6-11 所示。

表 6-10 业务策略信息列表——实例三

业务策略信息列表
5/97
1/1 第一页 上一页 下一页 最后页 前往 第 页
源起始端口 源结束端口 目的起始端口 目的结束端口 目的起始地址 目的结束地址 时间段 编辑
0 0 53 53 0.0.0.0 0.0.0.0 编辑
0 0 67 68 0.0.0.0 0.0.0.0 编辑
1 65535 80 80 0.0.0.0 0.0.0.0 worktime 编辑
0 0 0 0 0.0.0.0 0.0.0.0 freetime 编辑
0 0 0 0 0.0.0.0 0.0.0.0 编辑
全选 / 全不选
删除

表 6-11 业务策略信息列表（续表 6-10）——实例三

6.2.6.2 个人用户策略配置实例

如前所述，如果某个工作组中有个别用户的上网需求与该组其他用户基本相同，但同时也有少数一个或几个特别需求；或是某个用户突然有了新的上网需求时，就需要对这个用户单独定义业务策略。

例如，要求：允许“ Sale ”组（配置同上一节）的 WEB 业务，禁止该组的其他所有上网业务。特别地，允许该组 IP 地址为 192.168.16.66 的用户在时间段“ freetime ”的所有上网业务。

要配置的策略是：

生成策略 1，允许“ Sale ”组的 WEB 业务；系统会自动生成一条该组的全局策略 grp1_other，禁止所有业务；

生成策略 2，允许 IP 地址为 192.168.16.66 的用户的所有上网业务；该策略将自动位于策略 1 的上方。

当然，也可以先配置策略 2，再配置策略 1。不管配置顺序如何，在“ 业务策略信息列表 ”中，如表 6-12、6-13 所示，针对该用户的业务策略将始终位于针对“ Sale ”组的业务策略的上方。

表 6-12 业务策略信息列表——实例四

业务策略信息列表
5/97
1/1 第一页 上一页 下一页 最后页 前往 第 页
源起始端口 源结束端口 目的起始端口 目的结束端口 目的起始地址 目的结束地址 时间段 编辑
0 0 53 53 0.0.0.0 0.0.0.0 编辑
0 0 67 68 0.0.0.0 0.0.0.0 编辑
0 0 0 0 0.0.0.0 0.0.0.0 freetime 编辑
1 65535 80 80 0.0.0.0 0.0.0.0 worktime 编辑
0 0 0 0 0.0.0.0 0.0.0.0 编辑
全选 / 全不选
删除

表 6-13 业务策略信息列表（续表 6-12）——实例四

6.2.6.3 源端口的应用实例

一般情况下，业务策略是为了控制局域网主机的上网行为，因此无需设置参数“源起始端口”和“源结束端口”，HiPER 将自动开放所有源端口。上述两节中所提供的工作组和个人用户策略配置实例均是用来控制局域网主机的上网行为的。

但是，如果业务策略是为了限制 Internet 上的外网主机对局域网内部主机（比如某台服务器）的访问，就需要在该策略中指定“源起始端口”和“源结束端口”。

例如，要求：某网吧有一台游戏服务器（IP 地址为 192.168.16.200/24），现希望该服务器对外只提供某游戏服务（端口号为 7000、7100 和 7200，协议使用 TCP），并且只对它的另外两个连锁网吧开放（公网 IP 分别为：201.222.5.121/29 和 201.222.5.122/29）；同时，禁止该服务器的其他所有上网业务。要配置的相关策略是：

生成策略 1，允许该服务器的源端口 7000 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

生成策略 2，允许该服务器的源端口 7100 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

生成策略 3，允许该服务器的源端口 7200 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

生成策略 4，禁止该服务器的所有上网业务。

策略 1、2、3 的配置步骤类似，下面以策略 1 的配置步骤为例进行说明，如图 6-7 所示：

图 6-7 源端口的应用实例

第一步，在“策略名”中填入“1”；

第二步，在“组选择”中选择“新个人用户”，并在第一个下划线上填入“192.168.16.200”；

第三步，“协议”选择“6（TCP）”，“常用服务提示”选择“所有”；

第四步，在“目的起始地址”和“目的结束地址”中分别填入“201.222.5.121”、“201.222.5.122”；

第五步，在“源起始端口”和“源结束端口”中均填入“7000”；

第六步，“动作”选择“允许”；

第七步，单击“保存”按钮，该策略配置完成。

注意，在配置策略 2 和策略 3 时，在“组选择”中只需直接选择“192.168.16.200”即可。

策略 4 的配置步骤如下：

第一步，在“策略名”中填入“4”；

第二步，在“组选择”中选择“192.168.16.200”；

第三步，“协议”选择“所有”；

第四步，“动作”选择“禁止”；

第五步，单击“保存”按钮，该策略配置完成。

提示：还必须在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射***（章节 6.3.4 中）中为该服务器配置相关的 NAT 静态映射，该传奇服务器才能对外提供相关服务。

6.3　NAT 和 DMZ 配置

本节主要讲述 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置***的配置方法。

6.3.1 NAT 功能介绍

NAT（网络地址转换）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 日益短缺的问题，NAT 允许专用网络在内部使用任意范围的 IP 地址，而对于公用的 Internet 则表现为有限的公网 IP 地址范围。由于内部网络能有效地与外界隔离开，所以 NAT 也可以对网络的安全性提供一些保证。

HiPER 系列产品提供了灵活的 NAT 功能，具体特点如下所述：

6.3.1.1　NAT 地址空间

为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间：一个是局域网主机在内部使用的私有 IP 地址，HiPER 中用“ 内部 IP 地址 ”表示；另一个是用于外部的公网 IP 地址，HiPER 中用“ 外部 IP 地址 ”表示。

6.3.1.2　三种 NAT 类型

HiPER 提供三种 NAT 类型：“ EasyIP ”、“ One2One ”及“ Passthrough ”。

EasyIP：即网络地址端口转换，多个内部 IP 地址映射到同一个外部 IP 地址。它可为每个内部连接动态分配一个与单一外部地址有关的端口，并维护这些内部连接到外部端口的映射，从而实现多个用户同时使用一个公网地址与外部 Internet 进行通信。

One2One：即静态地址转换，内部 IP 地址与外部 IP 地址进行一对一的映射。它通常用来配置外网访问内网的服务器：内网服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

Passthrough：对指定的 IP 地址不做 NAT，直接按路由方式转发，它经常用于一些会受 NAT 影响制约的特别应用。比如，为保证 IP 语音和视频会议等应用的正常运行，可在内网中专门划分一个语音视频区，该区的主机均采用“ Passthrough ”方式。

我们将每个具体的 NAT 配置称为“ NAT 规则 ”，配置 NAT 规则时必须指定其出口 IP 地址及线路。当有多个合法的公网地址时，每种类型的 NAT 规则均可配置多个。实际应用中，常常需要混合使用不同类型的 NAT 规则。

6.3.1.3　主线路 NAT 规则和备份线路 NAT 规则

在 ***WEB 管理界面—>快速向导***（章节 3.2）中配置完上网接入线路（主线路），或者在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）中配置了主线路和备份线路后，系统会自动生成“ EasyIP ”类型的 NAT 规则，分别将它们称为主线路 NAT 规则和备份线路 NAT 规则。可以编辑修改它们，但不能删除。各种线路接入方式下，主线路 NAT 规则和备份线路 NAT 规则的名称如表 6-14 所示：

NAT 规则名	线路接入方式
PEBIND	主线路，PPPoE 拨号上网
ETHbind	主线路，固定 IP 接入
DYNAeth2	主线路，动态 IP 接入
PBIND	备份线路，PPPoE 拨号上网
IBIND	备份线路，固定 IP 接入
DYNA2eth3	备份线路，动态 IP 接入

表 6-14 主线路（备份线路）NAT 规则名称

负载均衡方式下，在 ***WEB 管理界面—>基本配置—>线路组合—>线路组合配置—>负载均衡***（章节 4.2.2.2）中配置主线路（备份线路）的“ 分配规则 ”、“ 权重 ”、“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”等参数，相当于在本页面配置主线路 NAT 规则（备份线路 NAT 规则）。相比之下，本页面提供更多的配置参数。

6.3.1.4　根据源地址指定优先通道

在这里，通道是指上网使用的 NAT 规则，它决定了上网使用的 NAT 类型、外部 IP 地址（即出口 IP）及线路。

HiPER 允许用户预先为局域网中的某些主机指定优先通道，它是通过设置 NAT 规则的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”来实现的，IP 地址属于两个地址范围内的主机将优先使用该 NAT 规则上网。对于已指定 NAT 规则的主机来说，当指定 NAT 规则可用时，它们只能使用该 NAT 规则上网；但是，当指定 NAT 规则失效时，HiPER 就把它们当作没有预先指定 NAT 规则的主机来处理。

6.3.1.5　根据线路带宽合理分配流量

HiPER 允许用户预先指定分配到两条线路的流量的比例，它是通过设置线路的“ 权重 ”来实现的。其中，线路的“ 权重 ”为绑定在该线路上的 NAT 规则的“ 权重 ”之和，需要注意的是，只有类型为“ EasyIP ”的 NAT 规则有“ 权重 ”。

在实际应用中，当局域网中的主机均未指定 NAT 规则时，可根据两条线路的带宽比来设置各线路的“ 权重 ”，从而实现按带宽分配流量。例如，主线路和备份线路的带宽分别为 6M、4M，若除了主线路 NAT 规则和备份线路 NAT 规则，还需配置一条绑定在主线路上的“ EasyIP ”NAT 规则，则可将主线路 NAT 规则、新配 NAT 规则、备份线路 NAT 规则的“ 权重 ”分别设为 2、1、2。这样，主线路、备份线路的“ 权重 ”就分别为 3、2，分配到主线路、备份线路的流量比将接近 3:2。

而当局域网中的某些主机指定了上网线路时，若按照带宽比来设置线路的“ 权重 ”，分配到两条线路的流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整“ 权重 ”。

6.3.1.6　两种流量分配规则

“ 分配规则 ”用来控制线路流量，它作用于局域网中没有预先指定 NAT 规则的计算机，HiPER 提供两种分配规则：“ NAT 会话 ” 和 “ IP 地址 ”，它们的实现机制如下所述。

1.　IP 地址

使用 IP 地址作为分配规则时，HiPER 将根据 NAT 规则的 “ 权重 ”，把未指定 NAT 规则的主机的 IP 地址，按顺序依次分配到各 “ EasyIP ” NAT 规则。分配到各 “ EasyIP ” NAT 规则的 IP 地址的数量比为它们的 “ 权重 ” 比，来自同一 IP 地址的 NAT 会话使用同一个规则。

例如，若共有三条 “ EasyIP ” NAT 规则，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用第一条规则，第 4、5 台主机将使用第二条规则，第 6 台主机将使用第三条规则，接着第 7、8、9 台主机将使用第一条规则，……，依此类推。注意，这里假设每台主机均只有一个 IP 地址。

2.　NAT 会话

使用 NAT 会话作为分配规则时，HiPER 将根据 NAT 规则的 “ 权重 ”，把未指定 NAT 规则的主机发起的 NAT 会话，按顺序依次分配到各“ EasyIP ”NAT 规则。分配到各“ EasyIP ” NAT 规则的 NAT 会话的数量比为它们的 “ 权重 ” 比，同一主机发起的 NAT 会话可使用多个 NAT 规则。

例如，若共有三条 NAT 规则，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，内网主机发起的第 1、2、3 个 NAT 会话将使用第一条规则，第 4、5 个 NAT 会话将使用第二条规则，第 6 个 NAT 会话将使用第三条规则，接着第 7、8、9 个 NAT 会话将使用第一条规则，……，依此类推。

一般情况下，建议 “ 分配规则 ” 选择为 “ IP 地址 ”。当对带宽要求高，需要双线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择 “ NAT 会话 ”，从而能够充分利用双线路带宽，以提高下载速度。需要注意的是，即便选择了 “ NAT 会话 ”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

6.3.1.7　NAT 静态映射

HiPER 集成了防火墙功能，通常情况下，广域网中的计算机无法通过 HiPER 访问局域网的某些服务器。HiPER 可提供 NAT 静态映射功能，通过定义一个服务端口，所有对 HiPER 该端口的服务请求将被重新定位给指定的局域网中的服务器。这样，广域网中的计算机就可实现对局域网服务器的访问。

6.3.1.8　虚拟服务器（DMZ 主机）

某些情况下，需要将一台局域网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机），被设置为虚拟服务器的计算机将失去 HiPER 的防火墙保护功能。当有外部用户访问为该 DMZ 主机分配的公网地址时，HiPER 会把数据包转发给指定的 DMZ 主机。

对于 HiPER 来说，当有多个公网 IP 地址时，可配置 1 个全局虚拟服务器，多个局部虚拟服务器。其中，局部虚拟服务器需指定其使用的 NAT 规则，该 NAT 规则的外部 IP 地址将分配给它；全局虚拟服务器则无需指定。局部虚拟服务器比全局虚拟服务器的优先级高，只有在没有配置局部虚拟服务器时，才使用全局虚拟服务器。

另外，NAT 静态映射的优先级高于虚拟服务器。当 HiPER 收到一个来自外部网络的请求时，它将首先根据外部请求所请求服务的端口号，查看 NAT 静态映射列表，检查是否有匹配的 NAT 静态映射，如果有的话，就把请求消息发送到该 NAT 静态映射对应的局域网计算机上去。如果没有匹配的静态映射，才会检查是否有匹配的虚拟服务器。

6.3.1.9　NAT 规则的执行顺序

当局域网中有主机发起 NAT 访问时，会首先检查此计算机是否符合所有 NAT 规则中“内部起始 IP 地址”到“内部结束 IP 地址”所指定的范围。如果有匹配的规则，则使用该条规则上网。如果没有匹配的规则，则使用“NAT 类型”为“EasyIP”的 NAT 规则上网；有多个“EasyIP”类型的 NAT 规则时，则根据“分配规则”为各条 NAT 规则分配流量，从而控制线路流量。

6.3.2 NAT 全局配置

图 6-8 NAT 全局配置

- 启用 NAT：打开或者关闭 NAT 功能，选中为打开；
- 分配规则：控制线路流量时使用的规则。选项：NAT 会话或 IP 地址，缺省值为 IP 地址；
- 最大 Session 数：局域网单个用户 NAT 最大并发连接数；
- 虚拟服务器（DMZ）：欲作为 DMZ 主机的局域网计算机的 IP 地址，此处配置的是全局虚拟服务器。
- 保存：NAT 全局配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 在配置完上网连接后，HiPER 会自动打开 NAT 功能。除非特别需要，请不要关闭此功能，否则 HiPER 将失去共享上网功能；

2. 当某些局域网应用（比如网络游戏）发生连接速度变慢的情况时，可以适当提高“最大 Session 数”。注意，“最大 Session 数”设置过高可能会导致 HiPER 减弱甚至丧失防止 DDoS 攻击的功能。

6.3.3 NAT 规则

6.3.3.1 NAT 规则配置

下面分别介绍“ EasyIP ”、“ One2One ”及“ Passthrough ”这三种类型的 NAT 规则的配置，如图 6-9、6-10、6-11 所示。

1. EasyIP

图 6-9 NAT 规则配置——EasyIP

- NAT 规则名：NAT 规则的名称（自定义，不能重复）。取值范围：1～11 个字符；
- NAT 类型：EasyIP；
- 外部 IP 地址：该 NAT 规则中，内部 IP 地址所映射的外部 IP 地址。主线路（备份线路）NAT 规则中，它显示为 0.0.0.0，表示默认使用当前端口地址，不能修改；配置其余本类型规则时，只能使用由 ISP 分配的 WAN 口（或 WAN2 口）以外的 IP 地址作为映射地址，不能为 0.0.0.0；
- 内部起始 IP 地址、内部结束 IP 地址：局域网中优先使用该 NAT 规则上网的计算机的起始 IP 地址和结束 IP 地址；
- 权重：该 NAT 规则的权重，取值范围为 1-255（整数），缺省值为 1；
- 虚拟服务器：欲作为 DMZ 主机的局域网计算机的 IP 地址，此处设置的是局部虚拟服务器，它只能使用该 NAT 规则。
- 绑定：
  主线路：该条 NAT 规则绑定在主线路上；
  备份线路：该条 NAT 规则绑定在备份线路上；
- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：配置 NAT 规则时，“ NAT 规则名 ”不能定义为“ PEBIND ”、“ ETHbind ”、“ DYNAeth2 ”、“ PBIND ”、“ IBIND ”和“ DYNA2eth3 ”这几个系统保留的 NAT 规则名。

2. One2One

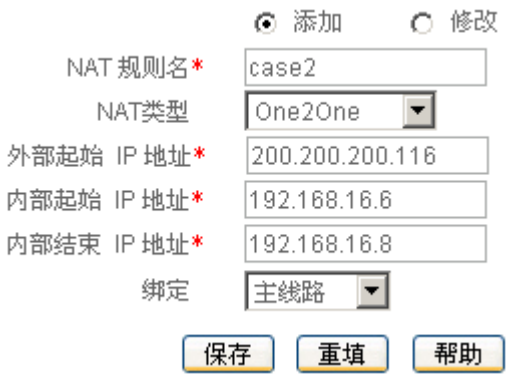


图 6-10 NAT 规则配置——One2One

“ NAT 规则名 ”、“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”、“ 绑定 ” 这几个参数的涵义同 “ EasyIP ” 方式中相关参数，这里不再重述，请参考相关描述。

- 外部起始 IP 地址：该 NAT 规则中，内部起始 IP 地址所映射的外部起始 IP 地址；
- NAT 类型：One2One。
- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：“ 外部起始 IP 地址 ”必须设置，实际映射的外部地址是从设置值开始向上依次增加。例如，如果 “ 内部起始 IP 地址 ” 设为 192.168.16.6，“ 内部结束 IP 地址 ” 设为 192.168.16.8，“ 外部起始地址 ” 设为 200.200.200.116，则 192.168.16.6、192.168.16.7、192.168.16.8 依次映射成 200.200.200.116、200.200.200.117、200.200.200.118。

3. Passthrough

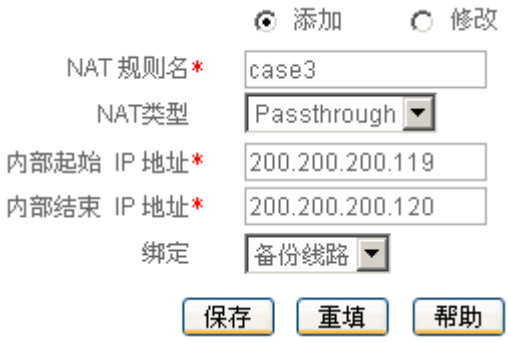


图 6-11 NAT 规则配置——Passthrough

“ NAT 规则名 ”、“ 绑定 ” 这两个参数的涵义同 “ EasyIP ” 方式中相关参数，这里不再重述，请参考相关描述。

- NAT 类型： Passthrough；
- 内部起始 IP 地址、内部结束 IP 地址：局域网中使用该 NAT 规则上网的计算机的起始和结束 IP 地址，这两个地址范围之内的 IP 地址不能与其他规则的外部 IP 地址重叠。
- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。

6.3.3.2　NAT 规则列表

表 6-15 NAT 规则信息列表

- 增加 NAT 规则：选中“ 添加 ”选项，输入 NAT 规则配置信息，单击“ 保存 ”按钮，生成新的 NAT 规则；
- 浏览 NAT 规则：如果已经生成了 NAT 规则，则可在“ NAT 规则列表 ”中浏览 NAT 规则信息，如表 6-15 所示；
- 编辑 NAT 规则：如果想编辑 NAT 规则，只需单击该条 NAT 规则后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 NAT 规则：选中一些 NAT 规则，单击右下角的“ 删除 ”按钮，即可删除被选中的 NAT 规则。

6.3.3.3　自定义 NAT 规则

第一步，确定所要配置的 NAT 规则的类型；

第二步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 配置***页面；

第三步，选择“ 添加 ”选项；

第四步，选择“ NAT 类型 ”为“ EasyIP ”、“ One2One ”或“ Passthrough ”。

第五步，分为三种情况：

如果“ NAT 类型 ”选择为“ EasyIP ”，依次填写“ 外部 IP 地址 ”、“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”、“ 权重 ”和“ 虚拟服务器 ”；

如果“ NAT 类型 ”选择为“ One2One ”，依次填写“ 外部 IP 地址 ”、“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”；

如果“ NAT 类型 ”选择为“ Passthrough ”，依次填写“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”；

第六步，选择“ 绑定 ”为“ 主线路 ”或“ 备份线路 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。可以在“ NAT 信息列表 ”中看到相应的记录；

第八步，继续配置其他 NAT 规则。

提示：

1. 删除 NAT 规则，在“ NAT 信息列表 ”中选中要删除的 NAT 规则，单击“ 删除 ”按钮，即可删除被选中的 NAT 规则；主线路 NAT 规则和备份线路 NAT 规则不能删除；

2. 系统自动生成的主线路（备份线路）NAT 规则的外部 IP 地址将显示为 0.0.0.0，表

示默认使用当前主线路（备份线路）端口，不能修改；其余自定义的 NAT 规则的外部 IP 地址不能为当前端口地址，也不能为 0.0.0.0；所有 NAT 规则的内部 IP 地址不能相互重叠，外部 IP 地址也不能相同；“ Passthrough ”类型的 NAT 规则的内部 IP 地址不能与另外两种类型的规则的外部 IP 地址重叠；

3. 在实际应用中，如果需要配置多条 NAT 规则，则在统一规划之后，应该首先配置或修改主线路（备份线路）NAT 规则，再配置其余自定义的 NAT 规则。如果已在 ***WEB 管理界面—>基本配置—>线路组合—>线路组合配置***（章节 4.2.2）中配置了主线路（备份线路）NAT 规则的相关参数，可直接在本页面修改它们；如果没有配置主线路（备份线路）NAT 规则的相关参数，可以在 ***WEB 管理界面—>基本配置—>线路组合—>线路组合配置***（章节 4.2.2）中进行快速配置，也可以直接在本页面进行配置。

例如，假设某用户已在 ***WEB 管理界面—>快速向导—>上网接入方式配置***(章节 3.2.4)中配置了上网主线路，ISP 分配了 2 个可用地址给主线路。现希望整个局域网用户分为两部分，一部分使用当前 WAN 口地址作为外部地址，即使用主线路 NAT 规则上网；另一部分使用 ISP 分配的另外一个地址作为外部地址。则必须首先将局域网用户根据 IP 地址划分为两组，同组内用户将使用同一条 NAT 规则上网；然后再在本页面配置主线路 NAT 规则的相关参数：“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”等，最后才能在本页面配置另一条 NAT 规则的相关参数。

6.3.3.4 NAT 规则配置的注意事项

HiPER 中，要保证 NAT 正常工作，还需注意以下事项，并进行相关配置。

1. 必须启用快速转发功能

配置方法为：进入 ***WEB 管理界面—>高级配置—>特殊功能—>快速转发***（章节 6.6.1）页面，启用快速转发功能。

2. 如果 WAN 口（或 WAN2/DMZ 口）为多地址接入，必须启用 NAT 类型的 ARP 代理功能

配置方法为：进入 ***WEB 管理界面—>基本配置—>端口配置***（章节 4 .4）页面，在 WAN 口（WAN 口多地址接入时）或者在 WAN2/DMZ 口（WAN2/DMZ 口多地址接入时）启用 NAT 类型的 ARP 代理功能。

3. 如果 WAN 口（或 WAN2/DMZ 口）为多地址接入，局域网主机要访问 ISP 分配的当前广域网端口 IP 地址之外的公网 IP 地址时，需配置相关的静态路由。

主要应用：

使用 EasyIP 类型的 NAT 规则的局域网主机要通过公网地址访问“ **One2One ”**类型的 NAT 规则所指定的内部主机时，需进入 ***WEB 管理界面—>高级配置—>路由配置***（章节 6.4）页面设置相关的静态路由。

一般情况下，相关的静态路由为主机路由，其目的地址为需要访问的公网地址，掩码为 255.255.255.255，网关为对应的广域网端口当前使用的 IP 地址。因此，如果需要访问多个 IP 地址，则需要设置多条主机路由。

当然，如果某些待访问的公网地址可以划分在同一个子网（该子网地址数更少，不能包括当前广域网端口 IP 地址）中，也可以通过为它们设置一条子网路由来实现：

其目的地址为新的子网的网络号，掩码为新的子网掩码，网关仍为对应的广域网端口当前使用的 IP 地址。

一般情况下，为避免无谓的错误，采用设置主机路由的方式即可。

6.3.3.5　NAT 规则配置实例

1.　EasyIP 方式应用实例

某网吧使用单线路上网，ISP 为该线路分配了八个地址：218.1.21.0/29 ~218.1.21.7/29，其中 218.1.21.1/29 是该线路的网关地址，218.1.21.2/29 是 HiPER 的 WAN 口 IP 地址。

现游戏 B 区（IP 地址范围：192.168.16.10/24~192.168.16.40/24）希望以 218.1.21.3/29 作为 NAT 映射地址通过 WAN 口上网，其对外虚拟服务器为 192.168.16.15，权重为 2。

配置步骤如下：

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 配置***页面；

第二步，单击“ 添加 ”按钮，如图 6-12 所示；

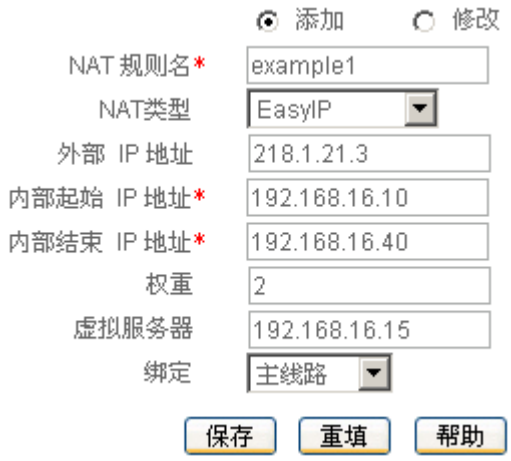


图 6-12 NAT 规则配置——实例一

第三步，在“ NAT 规则名 ”中填入 example1；

第四步，选择“ NAT 类型 ”为“ EasyIP ”；

第五步，在“ 外部 IP 地址 ”中填入 218.1.21.3；在“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.10 和 192.168.16.40；

第六步，在“ 权重 ”中填入 2，在“ 虚拟服务器 ”中填入 192.168.16.15；

第七步，选择“ 绑定 ”为“ 主线路 ”；

第八步，单击“ 保存 ”按钮，该条 NAT 规则配置成功。

2.　One2One 方式应用实例

1)　需求

如图 6-13 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽为 6M。电信给它分配了 5 个地址：202.1.1.130/29～202.1.1.1.134/29，使用电信提供的网关 202.1.1.129/29。

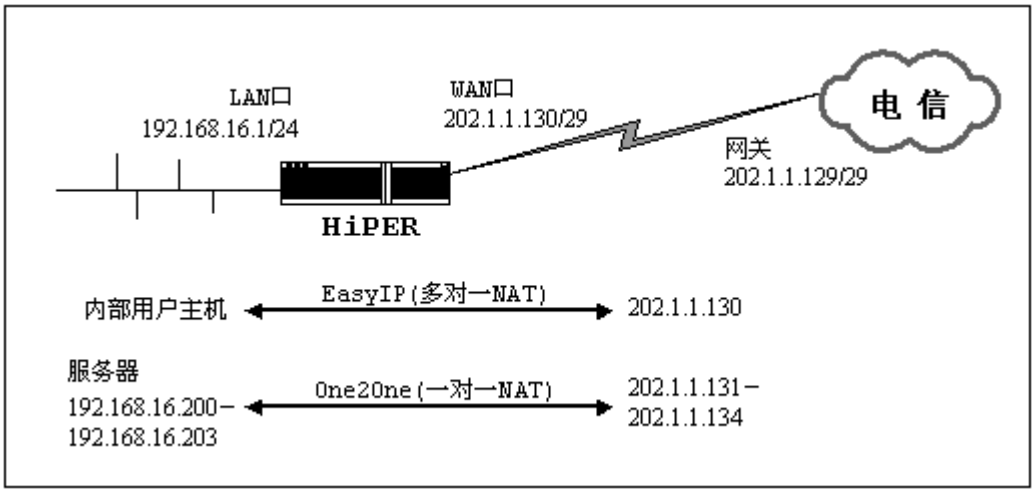


图 6-13 NAT 规则配置实例方案图——One2One 方式

该企业希望内部的人员上网通过 NAT 后使用 202.1.1.130/29 共享上网，另外有四台服务器做一对一 NAT（One2One）使用 202.1.1.131/29～202.1.1.1.134/29 对外提供服务。内部网络的地址是 192.168.16.0/24，4 台服务器的内部地址是 192.168.16.200/24～192.168.16.203/24。

2)　分析

由于该线路是采用固定 IP 接入方式上网，首先需要在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）页面中配置固定 IP 接入上网线路，或直接进入 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）页面中配置该线路。上网线路正确配置后，将自动生成主线路 NAT 规则，NAT 功能也自动启用。

而该企业使用提供四台内部服务器供外部访问，因此还需为它们设置一个类型为“One2One”的 NAT 规则。

最后，为保证 NAT 工作正常，还需进入 ***WEB 管理界面—>高级配置—>特殊功能—>快速转发***（章节 6.6.1）页面，启用快速转发功能；而由于 WAN 口是多地址接入，因此还需进入 ***WEB 管理界面—>基本配置—>端口配置***（章节 4.4）页面，在 WAN 口启用 NAT 类型的 ARP 代理功能；另外，如果局域网用户需要通过外部地址（202.1.1.131～202.1.1.134）访问内部服务器，还需设置相关的静态路由（具体方法参考章节 6.3.3.4）。

3)　One2One 类型的 NAT 规则配置

配置步骤如下：

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 配置***页面；

第二步，单击“添加”按钮，如图 6-14 所示；

图 6-14 NAT 规则配置——实例二

第三步，在“ NAT 规则名 ”中填入 example2；

第四步，选择“ NAT 类型 ”为“ One2One ”；

第五步，在“ 外部 IP 地址 ”中填入 202.1.1.131；在“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.200 和 192.168.16.203；

第六步，选择“ 绑定 ”为“ 主线路 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。

3. Passthrough 方式应用实例

1) 需求

如图 6-15 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽是 6M。电信提供给企业使用的连接地址为 202.96.97.2/30，电信使用的连接地址（即网关地址）为 202.96.97.1/30。该企业的内部用户主机将使用 202.96.97.2/30 共享上网，内部网络的地址是 192.168.16.0/24。

此外，电信还分配了一段地址给该企业使用，地址范围为 202.96.100.0/27~202.96.100.31/27，该企业将利用这些地址采用 Passthrough 方式配置多台服务器，对外提供服务；注意，202.96.100.0/27 和 202.96.100.31/27 分别为子网的子网号和广播地址，不可使用。

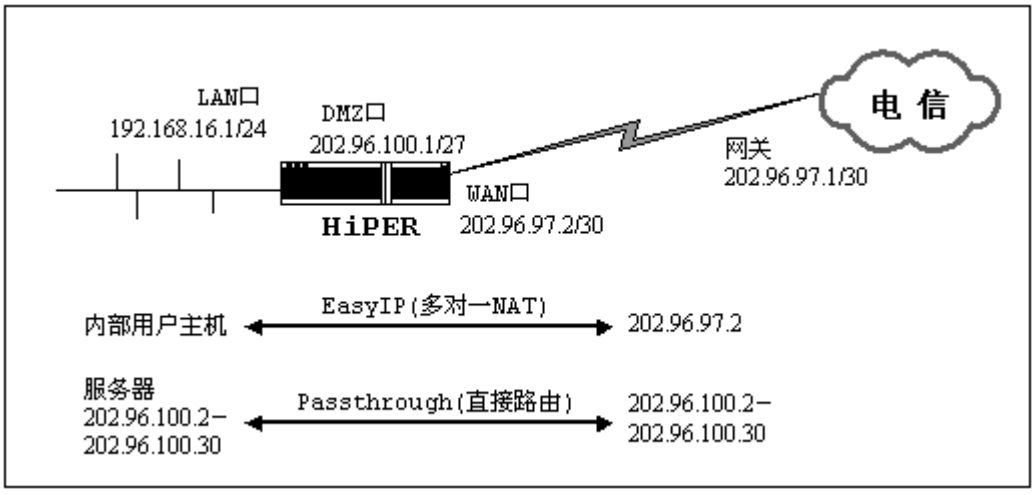


图 6-15 NAT 规则配置实例方案图——Passthrough 方式

2)　分析

由于该线路是采用固定 IP 接入方式上网，首先需要在 ***WEB 管理界面—>快速向导—>上网接入线路配置***（章节 3.2.4）页面中配置固定 IP 接入上网线路，或直接进入 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）页面中配置该线路。上网线路正确配置后，将自动生成主线路 NAT 规则，NAT 功能也自动启用。

另外，由于要求对外服务器采用 Passthrough 方式直接路由出网，因此，需将服务器通过交换机连接到 HiPER 的 WAN2/DMZ 口，将 DMZ 口的地址设为 202.96.100.1/27，并将服务器的地址设为 202.96.100.2/27~202.96.100.30/27 中的任一个，并且这些对外服务器的网关都是 202.96.100.1/27。之后，再为它们设置一个类型为“ Passthrough ”的 NAT 规则，地址范围为：202.96.100.2/27~202.96.100.30/27

最后，为保证 NAT 工作正常，还需进入 ***WEB 管理界面—>高级配置—>特殊功能—>快速转发***（章节 6.6.1）页面，启用快速转发功能

3)　Passthrough 类型的 NAT 规则配置

配置步骤如下：

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 配置***页面；

第二步，单击“ 添加 ”按钮，如图 6-16 所示；

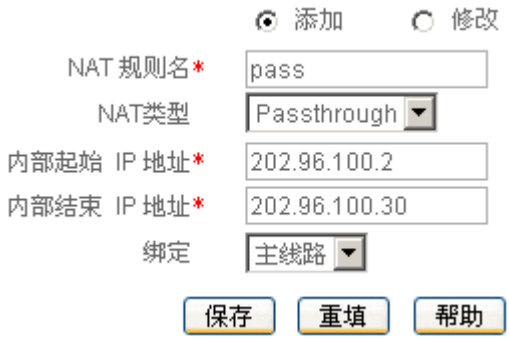


图 6-16 NAT 规则配置——实例三

第三步，在“ NAT 规则名 ”中填入 pass；

第四步，选择“ NAT 类型 ”为“ Passthrough ”；

第五步，在“ 内部起始 IP 地址 ”填入 202.96.100.2，和“ 内部结束 IP 地址 ”中填入 202.96.100.30；

第六步，选择“ 绑定 ”为“ 主线路 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。

6.3.4 NAT 静态映射

6.3.4.1 NAT 静态映射配置

图 6-17 NAT 静态映射配置

- NAT 静态映射名：NAT 静态映射的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 GRE；
- 外部起始端口：WAN 端的服务端口，即 HiPER 提供给 Internet 的服务端口；
- 内部 IP 地址：局域网中作为服务器的计算机的 IP 地址；
- 内部起始端口：局域网服务器所开服务的起始端口；
- 端口数量：从内部起始端口开始的一段连续的端口，最大设置为 20。例如：内部端口为 21，外部端口为 21，端口数量为 20，就代表内部端口范围为：21~40，同时外部端口与之一一对应，范围相应为：21~40；
- NAT 绑定：NAT 静态映射所绑定的 NAT 规则；选项为已配置的“ EasyIP ”类型的“ NAT 规则名 ”，代表相应的 NAT 规则；特别地，选项“ 主线路 ”和“ 备份线路 ”分别代表主线路 NAT 规则、备份线路 NAT 规则；
- 保存：NAT 静态映射配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 除“ TCP ”和“ UDP ”之外，对于其他类型的“ 协议 ”来说，“ 外部起始端口 ”、“ 内部起始端口 ”这三个参数必须设置为“ 0 ”，“ 端口数量 ”必须设置为“ 1 ”；

2. 系统某些功能会添加一些默认 NAT 映射（***WEB 管理界面—>系统管理—>远程管理***〈章节 5.8〉），在本页面无法删除它们。

6.3.4.2　NAT 静态映射列表

表 6-16 NAT 静态映射列表

- 增加 NAT 静态映射：选中“ 添加 ”选项，输入 NAT 静态映射信息，单击“ 保存 ”按钮，生成新的 NAT 静态映射；
- 浏览 NAT 静态映射：如果已经生成了 NAT 静态映射，可选择“ 显示 NAT 静态映射列表 ”选项，浏览 NAT 静态映射信息，如表 6-16 所示；
- 编辑 NAT 静态映射：如果想编辑 NAT 静态映射，只需单击此 NAT 静态映射后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 NAT 静态映射：选中一些 NAT 静态映射，单击右下角的“ 删除 ”按钮，即可删除被选中的 NAT 静态映射。

6.3.4.3　自定义 NAT 静态映射

第一步，进入 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射***页面；

第二步，选择“ 添加 ”选项，填写“ NAT 静态映射名 ”；

第三步，根据需要填写局域网服务器的“ 内部 IP 地址 ”，所开服务的“ 协议 ”和“ 内部起始端口 ”；

第四步，根据需要填写对外服务的“ 外部起始端口 ”，“ 外部起始端口 ”可以和“ 内部起始端口 ”不一致；

第五步，如果局域网服务器开设的服务是一段连续的端口，需要设置“ 端口数量 ”；

第六步，根据需要选择“ NAT 绑定 ”，绑定的 NAT 规则决定了映射的外部 IP 地址；

第七步，单击“ 保存 ”按钮，该 NAT 静态映射添加成功。可以在“ NAT 静态映射列表 ”中看到相应的记录；

第八步，继续配置其他的 NAT 静态映射。

提示：删除 NAT 静态映射，在“ NAT 静态映射列表 ”中选中要删除的 NAT 静态映射，单击“ 删除 ”按钮，即可删除被选中的 NAT 静态映射。

6.3.4.4　NAT 静态映射配置实例

1.　实例一

局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，但是希望外部通过 210 端口访问这个服务，具体配置如图 6-18 所示：

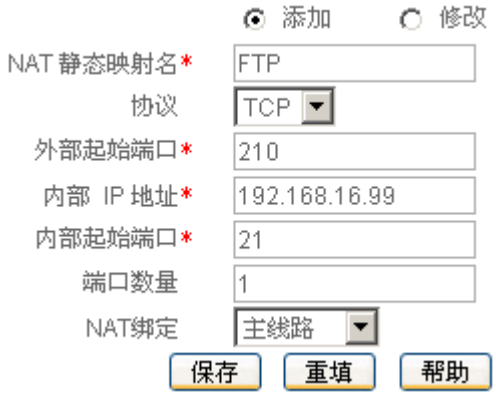


图 6-18 NAT 静态映射配置——实例一

2. 实例二

局域网计算机 192.168.16.100 开设了 UDP30000~UDP30019 端口的服务，希望可以映射到外部的 UDP30000~UDP30019 端口，则可将“ 端口数量 ”设为 20，具体配置如图 6-19 所示：

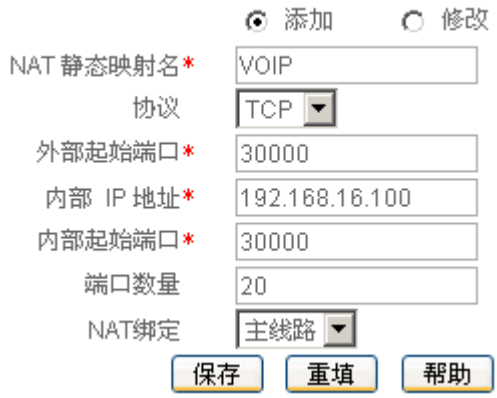


图 6-19 NAT 静态映射配置——实例二

3. 实例三

例如，ISP 分配了 218.1.21.0~218.1.21.7 八个地址，其中 218.1.21.1/29 是 HiPER 的网关地址，218.1.21.2/29 是 HiPER 的 WAN 口 IP 地址，局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，希望外部通过 218.1.21.3 的 TCP21 端口来访问这个服务。

首先需配置一条 NAT 规则，使其外部地址为 218.1.21.3，将其“ 规则名 ”设为“ example1 ”（具体配置参见 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 规则***〈章节 6.3.3〉中的配置实例）。然后再配置该 NAT 静态映射，“ NAT 绑定 ”选择“ example1 ”，具体配置如图 6-20 所示：

图 6-20 NAT 静态映射配置——实例三

6.4　路由配置

本节主要讲述 ***WEB 管理界面—>高级配置—>路由配置***的配置方法。

6.4.1 静态路由简介

6.4.1.1　静态路由

在本页面可配置静态路由，静态路由就是由网络管理员手工配置的路由，使得到指定目的网络的数据包的传送，按照预定的路径进行。静态路由不会随未来网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改路由表中相关的静态路由信息。

正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，比如实现流量控制、为重要的应用保证带宽等。

6.4.1.2　缺省路由

缺省路由是一种特殊的静态路由，简单地说，就是在没有找到匹配的路由时使用的路由。在路由表中，缺省路由以目的网络为 0.0.0.0、子网掩码为 0.0.0.0 的形式出现。如果数据包的目的地址不能与任何路由相匹配，那么系统将使用缺省路由转发该数据包。

在 ***WEB 管理界面—>快速向导***（章节 3.2）中配置完上网接入线路（主线路），或者在 ***WEB 管理界面—>基本配置—>ISP 配置***(章节 4.1.2)中配置了主线路和备份线路后，HiPER 会自动生成主线路（备份线路）的缺省路由，可在 ***WEB 管理界面—>系统状态—>路由和端口信息—>路由表信息列表***（章节 7.5.1）查看到对应路由信息，即目标地址为“ 0.0.0.0/0 ”的静态路由。

如果主线路（备份线路）为静态 IP 或动态 IP 上网方式时，还可在本页面的“ 路由信息列表 ”中查看到缺省路由的相关信息，参见表 6-17。

6.4.2 系统保留路由

系统提供几条保留的静态路由，具体信息参见表 6-17。其中，“ Detect ”和“ DetectDMZ ”的具体信息请参考 ***WEB 管理界面—>基本配置—>线路组合—>线路组合方式—>相关的静态路由***（章节 4.2.1.4）中的相关描述。用户自定义其他静态路由时，不允许使用系统的保留路由名。

路由名	端口/线路	性质	备注
Default	WAN/主线路	缺省路由	主线路为静态 IP 或动态 IP 上网方式时使用
DefaultDMZ	DMZ/备份线路	缺省路由	备份线路为动态 IP 上网方式时使用
IPETH	DMZ/备份线路	缺省路由	备份线路为静态 IP 上网方式时使用

DefaultLAN	LAN	缺省路由	LAN 口启用 DHCP 客户端功能时使用
Detect	WAN/主线路	静态路由	主线路启用线路检测时使用。当检测目标为“网关”时，无需使用。
DetectDMZ	DMZ/备份线路	静态路由	备份线路启用线路检测时使用。当检测目标为“网关”时，无需使用。

表 6-17 系统保留路由

6.4.3 静态路由配置

图 6-21 静态路由配置

- 路由名：静态路由的名称（自定义，不可重复）。取值范围：1~11 个字符；
- 目的网络：此条静态路由目的网络号；
- 子网掩码：此条静态路由目的网络的掩码；
- 网关地址：下一跳路由器入口的 IP 地址，HiPER 通过端口和网关定义一条跳到下一个路由器的线路。通常情况下，端口和网关须在同一网段；
- 检测间隔：同 ***WEB 管理界面—>基本配置—>线路组合***（章节 4.2）中的“检测间隔”，线路检测时发送检测包的时间间隔；
- 优先级：该路由的优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的路由转发数据包，值越低优先级越高；
- 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1。跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由，HiPER 会采用跳数值小的那条路由；
- 绑定：指定该静态路由的绑定端口，符合该静态路由的数据包将从指定端口转发。选项：主线路；备份线路；LAN-局域网端口；WAN-广域网端口；DMZ- DMZ/WAN2 端口；Blackhole-内部端口，转发到该端口的所有包都被 HiPER 丢弃；Local-内部软路由端口，转发到 HiPER 本身；Reject-内部端口，转发到该端口的所有包都被 HiPER 拒绝，并回应一个 ICMP 不可达；Loopback-回环地址，代表 127.0.0.0/8 网

段，不被转发。

- 保存：静态路由配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 如果不选择绑定端口，HiPER 将会自动选择一条最优路径，但是要设置转发到拨号连接上的必须手动指定；如果主线路或备份线路使用 PPPoE 拨号上网，相应地，“ 绑定 ”必须选择为“ 主线路 ”或“ 备份线路 ”；

2. 一般情况下，请不要修改“ Default ”、“ DefaultDMZ ”、“ IPETH ”、“ Detect ”及“ DetectDMZ ”这几条系统保留路由，以免上网异常。

6.4.4 路由列表

路由信息列表　5/100

1/1　第一页　上一页　下一页　最后页　前往 第 [ ] 页

	路由名	目的网络	子网掩码	网关地址	检测间隔	优先级	跳数	绑定	编辑
☐	Default	0.0.0.0	0.0.0.0	200.200.200.254	1000	60	1	eth2	编辑
☐	DefaultLAN	0.0.0.0	0.0.0.0	0.0.0.0	0	60	1		编辑
☐	DefaultDMZ	0.0.0.0	0.0.0.0	0.0.0.0	0	60	1		编辑
☐	Detect	0.0.0.0	0.0.0.0	0.0.0.0	0	60	1		编辑
☐	DetectDMZ	0.0.0.0	0.0.0.0	0.0.0.0	0	60	1		编辑

☐ 全选 / 全不选　删除

表 6-18 路由信息列表

- 增加静态路由：选中“ 添加 ”选项，输入静态路由信息，单击“ 保存 ”按钮，生成新的静态路由；
- 浏览静态路由：如果已经生成了静态路由，可以查看“ 路由信息列表 ”，如表 6-18 所示，浏览静态路由信息；
- 编辑静态路由：如果想编辑某条静态路由，只需单击此静态路由后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除静态路由：选中一些静态路由，单击右下角的“ 删除 ”按钮，即可删除被选中的静态路由。

6.4.5 自定义路由

第一步，进入 ***WEB 管理界面—>高级配置—>路由配置***页面；

第二步，选择“ 添加 ”选项，填入静态路由的名称；

第三步，输入该条路由指向的目的网段和子网掩码；

第四步，输入到该网段的下一跳路由器入口的 IP 地址；

第五步，如果需要监测线路状态，则需要设定检测间隔；

第六步，根据需要设置该条路由的优先级和路由跳数；

第七步，根据需要设置该条路由绑定的端口（如没有设置，HiPER 将自动选择最优路径，但是要设置转发到拨号连接上的必须手动指定）；

例如，到目的网段 192.168.1.0/24 的，设置了网关 192.168.16.254，则 HiPER 会自动选择路径，具体配置如图 6-22 所示。

图 6-22 路由参数设置——实例一

例如，到目的网段 218.19.213.45/32 的路由，其下一跳网关是 PPPoE 拨号所得的 IP 地址，这个地址并不是固定的，则必须选择绑定在主线路或备份线路上。注意：WAN 口的 PPPoE 线路选择绑定“ 主线路 ”，DMZ/WAN2 口的 PPPoE 线路选择绑定“ 备份线路 ”，具体配置如图 6-23 所示。

图 6-23 路由参数设置——实例二

第八步，单击“ 保存 ”按钮，该静态路由添加成功。可以在“ 路由信息列表 ”中看到相应的记录；

第九步，继续配置其他静态路由。

提示：若要删除路由，只需在“ 路由信息列表 ”中选中要删除的路由，单击“ 删除 ”按钮即可。

6.5　用户管理

本节主要讲述 ***WEB 管理界面—>高级配置—>用户管理***的配置方法。

6.5.1 用户管理功能介绍

6.5.1.1　用户管理概述

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权（业务管理）工作。在 ***WEB 管理界面—>高级配置—>业务管理***（章节 6.2）中，我们已经详细地介绍了如何实现对局域网用户上网行为的控制。在本节，我们将介绍如何解决用户的身份识别问题。

在用户管理中，通过 IP/MAC 地址绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址对作为用户唯一的身份识别标识，可以保护 HiPER 和网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到 HiPER 或者通过 HiPER。这台电脑的 IP 地址可以轻易地改变为受信任的地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

如图 6-24 所示，通过在“ 用户绑定配置 ”中添加可信的计算机的静态 IP 地址和对应的 MAC 地址，即可在“ 用户绑定信息列表 ”（表 6-19）中形成对应的 IP/MAC 地址对条目。

6.5.1.2　用户管理的工作原理

为方便起见，我们先介绍一下 HiPER 中，合法用户、非法用户及身份未知用户的概念。

合法用户：其 IP 地址及 MAC 地址与“ 用户绑定信息列表 ”中的某条目的 IP 地址与 MAC 地址完全匹配。

非法用户：其 IP 地址和 MAC 地址中有且只有一个与“ 用户绑定信息列表 ”中的某条目的 IP 地址或 MAC 地址匹配。

身份未知用户：即非 IP/MAC 绑定用户，其 IP 地址或 MAC 地址均不与“ 用户绑定信息列表 ”中的任何条目的 IP 地址或 MAC 地址匹配，也就是除合法用户以及非法用户之外的所有用户。

对于身份未知的用户，是在用户管理全局设置中统一控制的。如果选中“ 允许非 IP/MAC 绑定用户 ”，就表示允许这些用户连接或者通过 HiPER；如果没有选中“ 允许非 IP/MAC 绑定用户 ”，就表示禁止这些用户连接或者通过 HiPER。

IP/MAC 绑定应用于来自于局域网内部，连接到 HiPER 的数据包或者通过 HiPER 上网的数据包。当局域网用户有数据流量连接和通过 HiPER 时，将首先和“ 用户绑定信息列表 ”中的条目相比较，即进行身份识别；之后，根据用户身份的不同，来自该用户的数据包将被丢弃或进入 IP 业务管理功能模块处理（即继续去匹配业务策略）。具体描述如下：

1. 如果该用户是合法用户，则允许该数据包通过，并继续去匹配业务策略；
2. 如果该用户是非法用户，则丢弃该数据包；
3. 如果该用户身份未知，则根据用户管理全局设置执行：

1) 若允许身份未知用户，即在全局设置中，选中“ 允许非 IP/MAC 绑定用户 ”时，则允许该数据包通过，并继续去匹配业务策略；
2) 若禁止身份未知用户，即在全局设置中，没有选中“ 允许非 IP/MAC 绑定用户 ”时，则丢弃该数据包。

例如，如果某用户 IP/MAC 地址 192.168.16.221 和 00:22:aa:00:22:bb 已经添加到“ 用户绑定信息列表 ”，如表 6-19 所示：

表 6-19 用户绑定信息列表——实例一

那么，当 HiPER 接收到来自局域网的数据包时，将会根据以下几种情况处理：

1. 一个 IP 地址为 192.168.16.221，MAC 地址为 00:22:aa:00:22:bb 的数据包将被允许通过，并继续去匹配业务策略；
2. 一个 IP 地址为 192.168.16.221，但是使用了其他 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击；
3. 一个使用了其他 IP 地址，但是 MAC 地址是 00:22:aa:00:22:bb 的数据包也将被丢弃，以防止 IP 欺骗；
4. 如果这个数据包的 IP 地址和 MAC 地址在“ 用户绑定信息列表 ”都没有定义：
   1） 如果选中“ 允许非 IP 和 MAC 绑定用户 ”，则允许该数据包通过，并继续去匹配业务策略。
   2） 如果没有选中“ 允许非 IP 和 MAC 绑定用户 ”，则禁止该数据包通过。

注意，在启用了 IP/MAC 绑定功能之后，如果修改了一台电脑的 IP 地址或者 MAC 地址，而且此 IP 地址和 MAC 地址已经在“ 用户绑定信息列表 ”中，则必须同时修改“ 用户绑定信息列表 ”中的相应的条目。否则这台电脑将无法访问 HiPER 或者通过 HiPER。当未选中“ 允许非 IP/MAC 绑定用户 ”时，如果希望局域网中新增的主机可以访问或通过 HiPER，则必须为该主机在“ 用户绑定信息列表 ”中添加 IP/MAC 绑定地址对。

用户管理功能只能影响用户访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该 HiPER 的通信）。如果用户修改了 IP 或 MAC，将不能访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但是不能影响局域网内部通信，比如网络邻居浏览。

6.5.2 IP 和 MAC 绑定用户配置

图 6-24 IP 和 MAC 地址绑定用户配置

图 6-25 ARP 表信息

- 用户名：欲进行 IP 和 MAC 地址绑定的用户名称。自定义，不能重复，取值范围：1～31 个字符；
- IP 地址：该用户的 IP 地址（可使用 ipconfig /all 命令获得）；
- MAC 地址：该用户的 MAC 地址（可使用 ipconfig /all 命令获得）。
- 保存：IP/MAC 绑定用户配置参数生效；
- 重填：恢复到修改前的配置参数。
- 读 ARP 表：显示当前的动态 ARP 映射条目，即 HiPER 通过 LAN 口动态学习到的用户的 ARP 信息。注意，如果已经将某用户的 IP/MAC 地址对添加到“ 用户绑定信息列表 ”中，该用户的 IP/MAC 地址对将不再显示。

提示：可以通过动态 ARP 列表来添加用户。如图 6-25 所示，双击欲绑定的 IP/MAC 地址对，比如 200.200.200.139（00:07:95:a8:1c:3d），即可将之添加到配置页面中（如图 6-26），此时，用户名将显示为 IP 地址。然后，单击“ 保存 ”按钮，即可将之添加到“ 用户绑定信息列表 ”中。

图 6-26 IP 和 MAC 地址绑定用户配置——实例 1

6.5.3 用户管理全局设置

图 6-27 用户管理全局设置

- 允许非 IP/MAC 绑定用户：允许或禁止非 IP/MAC 绑定用户连接到 HiPER。
- 保存：用户管理全局配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：当决定取消“ 允许非 IP/MAC 绑定用户 ”功能前，必须确认管理计算机已经被添加到“ 用户绑定信息列表 ”中，否则将会造成管理计算机无法连接到 HiPER 的现象。

6.5.4 用户绑定信息列表

表 6-20 用户绑定信息列表

- 增加 IP 和 MAC 绑定用户：选中“ 添加 ”选项，输入 IP 和 MAC 绑定信息，单击“ 保存 ”按钮，生成新的 IP 和 MAC 绑定用户；
- 浏览 IP 和 MAC 绑定用户：如果已经生成了 IP 和 MAC 绑定用户，可以查看“ 用户绑定信息列表 ”（如表 6-20），浏览 IP 和 MAC 绑定用户信息；
- 编辑 IP 和 MAC 绑定用户：如果想编辑某个 IP 和 MAC 绑定用户，只需单击此 IP 和 MAC 绑定用户后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 IP 和 MAC 绑定用户：选中一些 IP 和 MAC 绑定用户，单击右下角的“ 删除 ”按钮，即可删除被选中的 IP 和 MAC 绑定用户。

6.5.5 自定义 IP 和 MAC 绑定用户

配置 IP 和 MAC 绑定用户的步骤如下：

第一步，进入 ***WEB 管理界面—>高级配置—>用户管理***页面；

第二步，选择“ 添加 ”选项，输入该用户的“ 用户名 ”（自定义）、“ IP 地址 ”和“ MAC 地址 ”，然后单击“ 保存 ”按钮；

第三步，该 IP 和 MAC 绑定用户添加成功后，可以在“ 用户绑定信息列表 ”中看到相

应的条目，对于匹配该条目的数据包，将被允许连接或者通过 HiPER。如果在 ***WEB 管理界面—>高级配置—>业务管理***（章节 6.2）中为该用户配置了业务策略，这些数据包还将继续去匹配这些业务策略；

第四步，继续配置其他 IP 和 MAC 绑定用户；

第五步，如果要禁止身份未知的用户，即“用户绑定信息列表”以外的用户，连接或者是通过 HiPER，则需取消“允许非 IP/MAC 绑定用户”的选中，然后单击“保存”按钮。否则的话，身份未知的用户也将被允许连接或者是通过 HiPER。

当配置完 IP/MAC 绑定之后，所有能正常连接到 HiPER 的数据包将首先和“用户绑定信息列表”中的条目相比较。然后根据相关配置，该数据包将被禁止或进入 IP 业务管理功能模块处理。

提示：若要删除 IP/MAC 绑定用户，在“用户绑定信息列表”中选中要删除的 IP/MAC 绑定用户，单击“删除”按钮即可。

6.5.6 配置上网“白名单”和“黑名单”

灵活地运用 IP/MAC 绑定功能，可以为局域网用户配置上网“白名单”和“黑名单”。

通过配置上网“白名单”，将只允许“白名单”中的用户通过 HiPER 上网，禁止其他所有用户通过 HiPER 上网。因此，如果要求只允许局域网中的少数用户上网，可通过配置上网“白名单”来实现。

通过配置上网“黑名单”，将只禁止“黑名单”中的用户通过 HiPER 上网，允许其他所有用户通过 HiPER 上网。因此，如果要求只禁止局域网中的少数用户上网，可通过配置上网“黑名单”来实现。

在 HiPER 中，“白名单”中的用户即为合法用户——其 IP 地址及 MAC 地址与“用户绑定信息列表”中的某条目的 IP 地址与 MAC 地址完全匹配。“黑名单”中的用户即为非法用户——其 IP 地址和 MAC 地址中有且只有一个与“用户绑定信息列表”中的某条目的 IP 地址或 MAC 地址匹配。

6.5.6.1 配置上网“白名单”

为局域网用户配置上网“白名单”，步骤如下：

第一， 通过配置 IP/MAC 地址绑定对来指定合法用户，将具有上网权限的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，并添加到“用户绑定信息列表”中。

第二， 不选中“允许非 IP/MAC 绑定用户”，其他所有不在“用户绑定信息列表”中的主机将不能上网。

6.5.6.2 配置上网“黑名单”

为局域网用户配置上网“黑名单”，步骤如下：

第一， 通过配置 IP/MAC 地址绑定对来指定非法用户，有两种方法：将禁止上网的主机的 IP 地址和任意一个非本局域网网卡的 MAC 地址作为 IP/MAC 地址绑定对，并添加到“用户绑定信息列表”中；或将禁止上网的主机的 MAC 地址和任意一个非本局域网网段

的 IP 地址作为 IP/MAC 地址绑定对，并添加到“ 用户绑定信息列表 ”中。

第二， 选中“ 允许非 IP/MAC 绑定用户 ”，其他所有 IP 地址和 MAC 地址均不在“ 用户绑定信息列表 ”中的主机将能够上网。

例如，如果要禁止具有某个 MAC 地址（例如 00:22:44:00:22:44）的主机连接和通过 HiPER，可以添加一个 IP/MAC 地址绑定对，输入该 MAC 地址，而 IP 地址则设置成一个任意的非本局域网网段的 IP 地址，如表 6-21 所示。

表 6-21 用户绑定信息列表——实例二

例如，如果要禁止具有某个 IP 地址（例如 192.168.16.100）的主机访问和连接 HiPER，可以添加一个 IP/MAC 地址绑定对，输入该 IP 地址，而 MAC 地址则设置成任意一个非本局域网网卡的 MAC 地址，如表 6-22 所示。

表 6-22 用户绑定信息列表——实例三

6.6　特殊功能

本节主要讲述 ***WEB 管理界面—>高级配置—>特殊功能***的配置方法。

快速转发功能，是通过使用转发缓存来简化分组的转发操作，从而提高分组转发速率和转发的吞吐量。在快速转发过程中，只需对一组具有相同目的地址和原地址的分组的前几个分组进行传统的路由转发处理，并把成功转发的分组的目的地址、源地址和下一网关地址（下一路由器地址）放入转发缓存中。当其后的分组要进行转发时，会首先查看转发缓存，如果该分组的目的地址和源地址与转发缓存总的匹配，则直接根据转发缓存中的下一网关地址进行转发，而无须经过传统的复杂操作，大大减轻了路由器（网关）的负担，达到了提高路由器吞吐量的目标。

内网主机速率限制功能，是通过限制内网主机的下载速率和上传速率，从而控制上传和下载的流量。利用速率限制，系统管理员可以控制输出和输入流量的速率，以确保用户或者应用不会超过所分配的最大传输速率，或者独占网络带宽。结合 HiPER 的带宽管理功能，速率限制有助于控制网络拥塞，避免少数用户上下载大型文件时可能会导致的网络速度急剧下降，保证实时应用（如 IP 电话和视频会议）的质量。

虚拟局域网（VLAN）是一种通过将局域网内的设备逻辑地址而不是物理地址划分成一个个网段从而实现虚拟工作组的技术，一个 VLAN 组成一个逻辑子网，即一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信；不同的 VLAN 之间实现物理隔离，一个 VLAN 内部的单播、广播和多播包都不会转发到其他 VLAN 中，从而有助于控制流量、简化网络管理、加强网络安全性。HiPER 可实现基于端口的虚拟局域网（VLAN），将 LAN 口（集成 4 端口以太网交换机）的 4 个端口设置成不同的组号，相同组号的端口即构成一个 VLAN。

端口镜像功能可将交换机的其他端口的流量自动复制到镜像端口，实时提供各端口的传输状况的详细资料，以便网络管理人员进行流量监控、性能分析和故障诊断。HiPER 中，LAN 口的端口 1 为镜像端口。由于 HiPER 的端口镜像功能完全由硬件提供，因此不会影响 HiPER 的性能、速度以及各个应用功能。

6.6.1 快速转发

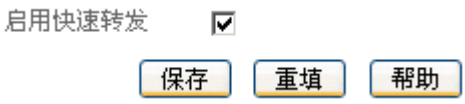


图 6-28 启用快速转发

- 启用快速转发：启用或者是关闭快速转发，选中是启用。快速转发功能可以实现各个物理端口数据的快速转发，全面提高性能。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：如果需要使用 CBQ 带宽业务管理功能（在 ***WEB 管理界面—>带宽业务***〈章节 9〉中配置），必须关闭快速转发。

6.6.2 内网主机速率限制

图 6-29 内网主机速率限制

- bps：bit/s，内网主机每秒传送的最大比特数，取值范围为 64K-100M；特别地，选项“ NoLimit ”表示不限制，“ Block ”表示禁止传送；
- pps：packet/s，内网主机每秒传送的数据包的最大数量，取值范围为 0-65535，0 表示不限制。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 在此处可以限制内网主机的下载速率和上传速率，从而控制上传和下载的流量。上传的方向是指数据从内网主机出发经过 HiPER 到外网，下载的方向正好相反。

2. 若设置了上传速率或下载速率，则内网任一主机的相应参数值都不可能超过设置值。

6.6.3 虚拟局域网

图 6-30 虚拟局域网

- 端口 1 组号—端口 4 组号：LAN 口的 4 个交换口可以配置不同的组号，相同组号的端口在一个交换机广播域内，不同组号的端口之间相互隔离。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 相同组号的端口构成一个虚拟局域网（即 VLAN），同一 VLAN 中的端口可互相连通；不同 VLAN 之间的端口，相当于硬件隔离，不能相互通信；

2. 缺省情况下所有端口都属于同一个 VLAN，最复杂情况每个端口分别属于不同的 VLAN。如图 6-30 中，表示端口 1 和端口 2 同属一个 VLAN（组号均为 1），端口 3、端口 4 分别各属一个 VLAN。

6.6.4 端口镜像

图 6-31 启用端口镜像

- 启用端口镜像：启用或者是关闭端口镜像，选中是启用。HiPER 中，LAN 口的端口 1 实现端口镜像的功能，端口 2、3、4 的流量将镜像到端口 1，以便进行流量和协议分析，提供诊断便利。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：如果 LAN 口的 4 个端口不在同一个虚拟局域网内，那么只有与端口 1 同属一个虚拟局域网的端口的流量才能镜像到端口 1。

6.6.5 端口镜像应用

传统方式下，为实现对网吧或企业内部流量得监控和管理，一般是在 HiPER 下再接一台 HUB，而 HUB 是共享型网络设备，放在总出口，无疑会大大降低网络速度，造成网络瓶颈。如果采用 HiPER，则只需将监控主机直接连到 LAN 口的端口 1，如图 6-32 所示，再在 ***WEB 管理界面—>高级配置—>特殊功能—>端口镜像***（章节 6.6.4）中启用端口镜像功能，即可在监控主机上监控到整个局域网的流量。

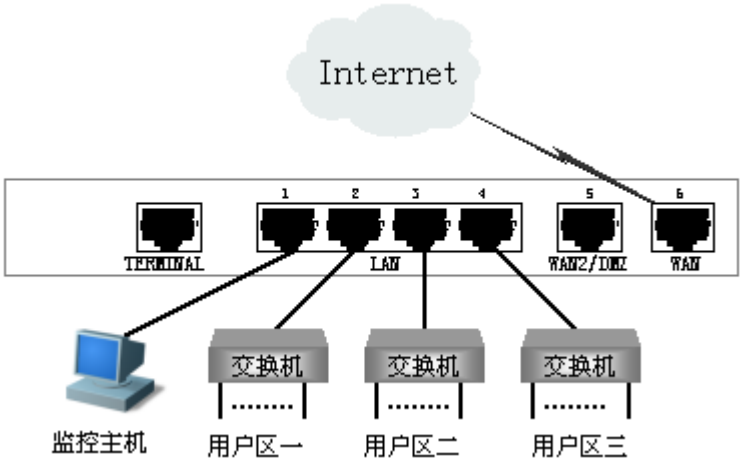


图 6-32 端口镜像应用

第7章　系统状态

系统状态里面记载了 HiPER 中运行的大量状态信息，通过查看、分析这些运行信息，对于管理员分析系统的状况、监视路由器的活动来说，是一个相当重要的部分。

HiPER 在 NAT 的环境下，提供强大的监控功能，主要分为两类：一类是分类统计，可以帮助管理员发现过去网络运行中出现过的问题；另一类是在线监控，可以帮助管理员分析目前网络运行中哪个主机出现了问题，出现了何种问题，以及对其他主机造成的影响。

HiPER 的运行状态管理分为三个层次：

物理状态：端口物理状态信息以及收发数据包信息，路由表信息等；

用户状态：每一个局域网用户的信息，包括收发包信息、带宽占用情况等；

NAT 状态：针对 NAT 的特别信息，帮助管理员发现用户在使用 Internet 过程中发生的 DDoS 攻击，巨量下载，过分占用 Internet 带宽等情况。

7.1　用户统计

本节主要讲述 ***WEB 管理界面—>系统状态—>用户统计***的使用。

通过“ 用户统计信息列表 ”，可以查看内网各主机的上网流量信息；同时，该表还具有排序功能，针对表中的每个参数，均可把所有信息条目按照该参数值的大小排序，排序顺序可以是从小到大，也可以是从大到小。

用户统计信息列表　　35/35

1/2　第一页　上一页　下一页　最后页　前往 第 [ ] 页

ID	用户名	IP地址	MAC地址	活动记录	接收数据包	发送广播包	发送数据包	广播包 / 发送包
1		200.200.200.175	00:22:aa:00:22:aa	0:00:00:01	77966	168	97244	0%
2		0.0.0.0	02:01:00:00:00:00	0:00:00:00	0	2612	0	0
3		200.200.200.15	00:e0:4c:e0:47:0f	0:00:00:00	69994	249	79635	0%
4		200.200.200.207	00:22:aa:bb:cc:ee	0:00:01:14	9107	282	11561	3%
5		200.200.200.131	00:20:e0:71:e0:40	0:00:00:00	69681	262	73072	0%
6		200.200.200.213	00:0f:1f:a4:bf:21	0:00:00:00	145278	585	7137	0%
7		200.200.200.50	00:0a:e6:f6:2f:0a	0:00:13:03	12	0	7	0
8		200.200.200.212	00:20:e0:70:11:eb	0:00:00:01	3996	148	5064	4%
9		200.200.200.198	00:22:aa:3d:ff:38	0:00:00:48	44863	48	47997	0
10		100.100.100.1	00:22:aa:13:d6:3e	0:00:02:56	0	132	0	0
11		200.200.200.227	00:e0:4c:40:76:ef	0:00:00:00	671682	1284	21908	0%
12		200.200.200.208	00:20:e0:70:91:57	0:00:00:00	14046	376	15901	3%
13		192.168.16.1	00:22:aa:ff:ff:ff	0:00:00:04	0	64	0	0
14		200.200.200.201	00:e0:4c:3c:d3:38	0:00:00:03	18710	715	20587	4%
15		200.200.200.55	00:22:aa:13:d6:33	0:00:00:02	9575	134	4098	1%
16		200.200.200.223	00:0d:87:0d:58:5f	0:00:00:06	13491	793	15534	6%
17		200.200.200.108	00:22:aa:13:e1:f6	0:00:00:11	7388	27	8676	0
18		200.200.200.151	00:22:aa:35:8f:bd	0:00:00:38	0	9	0	0
19		200.200.200.150	00:10:5c:af:27:56	0:00:02:52	196	154	109	79%
20		200.200.200.54	00:22:aa:3e:98:bc	0:00:00:03	44737	179	30263	0%

清除　刷新

表 7-1 用户统计信息列表

- ID：序号；
- 用户名：某用户计算机（NetBIOS）名；
- IP 地址：内网用户的 IP 地址信息；
- MAC 地址：内网用户的 MAC 地址信息；
- 活动记录：某用户上一次通过 HiPER 发送或接收数据包距离查询时刻的时间；
- 发送数据包：某用户向 HiPER 发送的单播包的数量，一般是该用户上网时向 Internet 发送的数据包；
- 发送广播包：某用户向 HiPER 发送的广播包（包括多播包）的数量；
- 接收数据包：HiPER 向某用户发送的单播包的数量，一般是该用户上网时从 Internet 下载的数据包；
- 广播包/发送包：某用户向 HiPER 发送的广播包（包括多播包）和单播包的数量比。
- 清除：单击“ 清除 ”按钮，可将“ 用户统计信息列表 ”全部信息清除，配合刷新按钮，可查看清除时刻至今这段时间内的用户统计信息。
- 刷新：单击“ 刷新 ”按钮，可以看到“ 用户统计信息列表 ”的最新信息。
- 排序：单击标题栏中的某个参数，所有信息条目将按照该值的大小排序，方向为从小到大；再次单击该参数，排序方向将变为从大到小。例如，如果单击“ 发送数据包 ”，则表里的所有信息条目将按照“ 发送数据包 ””的值从小到大排序，如果再次单击“ 发送数据包 ””，排序方向将变为从大到小。

提示：

1. 发现内网流量最大的用户：上表中发送数据包或者广播包一列中数量最大的用户（例如表 7-1 中 ID 为 1 的用户）；

2. 一般来说，计算机在开机的时候会发送一些广播包，某些软件在运行的时候也会发送一些广播包，计算机运行一段时间后（一般是开机运行 20 分钟后或上网 10 分钟后，开始考量这个数值），其发送广播包的数量应该小于单播包数量的 10%，如果比例远大于 10%，该计算机可能感染了病毒；

3. 某些软件（如网吧计费管理软件）在使用的时候会发送大量的广播包，这时“ 广播包/发送包 ”将远大于 10%，此时应该忽略这种异常情况；

4. 如果在“ 用户统计信息列表 ”里面看到 IP 地址为 0.0.0.0 的用户（例如表 7-1 中 ID 为 2 的用户），这些用户是一些只发送广播包而没有和 HiPER 通讯过的网络设备。这样 HiPER 只能识别出它的 MAC 地址，而不能识别 IP 地址。这些网络设备可能来自局域网，也可能来自广域网（ISP 采用 LAN 形式为用户提供接入线路），当它们发送的广播包过高时，会造成 HiPER 的端口的拥塞，网速变慢。

7.2　NAT 统计

本节主要讲述 ***WEB 管理界面—>系统状态—>NAT 统计***的使用。

NAT 统计页面包括“ NAT 状态信息列表 ”（如表 7-2）和“ NAT 统计信息列表 ”（如表 7-3、7-4）。

7.2.1 NAT 状态信息列表

NAT状态信息列表 7/7

1/2 第一页 上一页 下一页 最后页 前往 第 页

ID	起始IP	结束IP	外部IP	类型	虚拟服务器	端口	权重	选择计数	租期
1	192.168.16.40	192.168.16.100	200.200.200.114	EasyIP	192.168.16.50	ie1	2	208	0:01:18:30
2	192.168.16.110	192.168.16.140	0.0.0.0	EasyIP	192.168.16.120	ptpdial0	1	0	0:01:18:30
3	192.168.16.10	192.168.16.30	200.200.200.115	EasyIP	192.168.16.15	ie1	1	0	0:01:18:30
4	192.168.16.6	192.168.16.6	200.200.200.116	One2One	192.168.16.6	ie1	0	0	0:01:18:30
5	192.168.16.7	192.168.16.7	200.200.200.117	One2One	192.168.16.7	ie1	0	0	0:01:18:30

刷新

表 7-2 NAT 状态信息列表

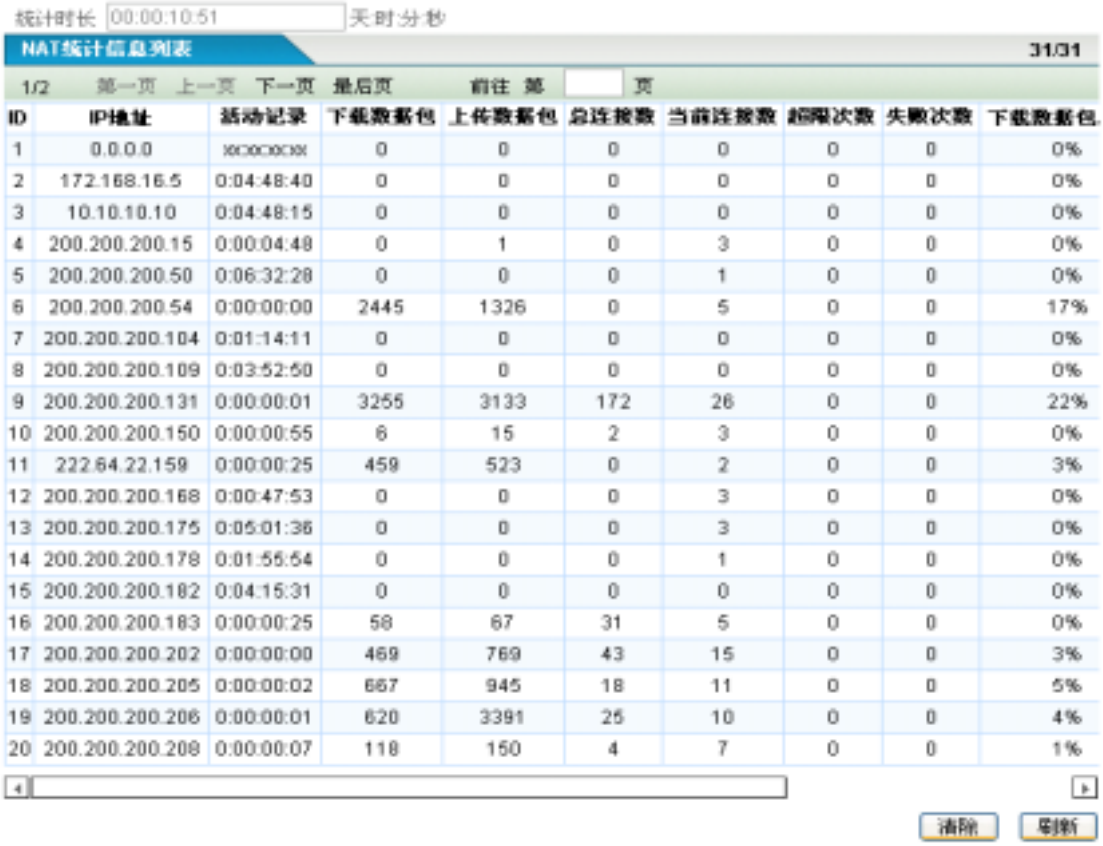
- ID：序号；
- 起始 IP、结束 IP：该 NAT 规则设置的起始 IP 地址和结束 IP 地址；
- 类型：该 NAT 规则的类型，可以是 EasyIP、One2One 或 Passthrough；
- 虚拟服务器：该 NAT 规则设置的虚拟服务器，它通过该 NAT 规则上网；
- 端口：该 NAT 规则所绑定线路的端口名称，可以是物理端口 ie0（即 LAN）、ie1（即 WAN）、ie2（即 DMZ/WAN2）或者是虚端口；
- 权重：该 NAT 规则的权重值；
- 选择计数：在“ 租期 ”这段时间内，使用该 NAT 规则的 NAT 会话的累计数量。如果该 NAT 规则未生效或未被使用，则该值为 0；
- 租期：该 NAT 规则上一次状态变化距离查询时刻的时间。

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的“ NAT 状态信息列表 ”。

提示 :同 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置***(章节 6.3.3) 中的‘ NAT 信息列表 ”相比，在这里将“ One2One ”类型的 NAT 规则进行了细分，一个外部地址对应一条记录。

7.2.2 NAT 统计信息列表

通过“ NAT 统计信息列表 ”，可以查看内网各主机的 NAT 统计信息；同时该表还具有排序功能，针对表中的每个参数，均可把所有信息条目按照该参数值的大小排序，排序顺序可以是从小到大，也可以是从大到小。



统计时长 00:00:10:51 天:时:分:秒

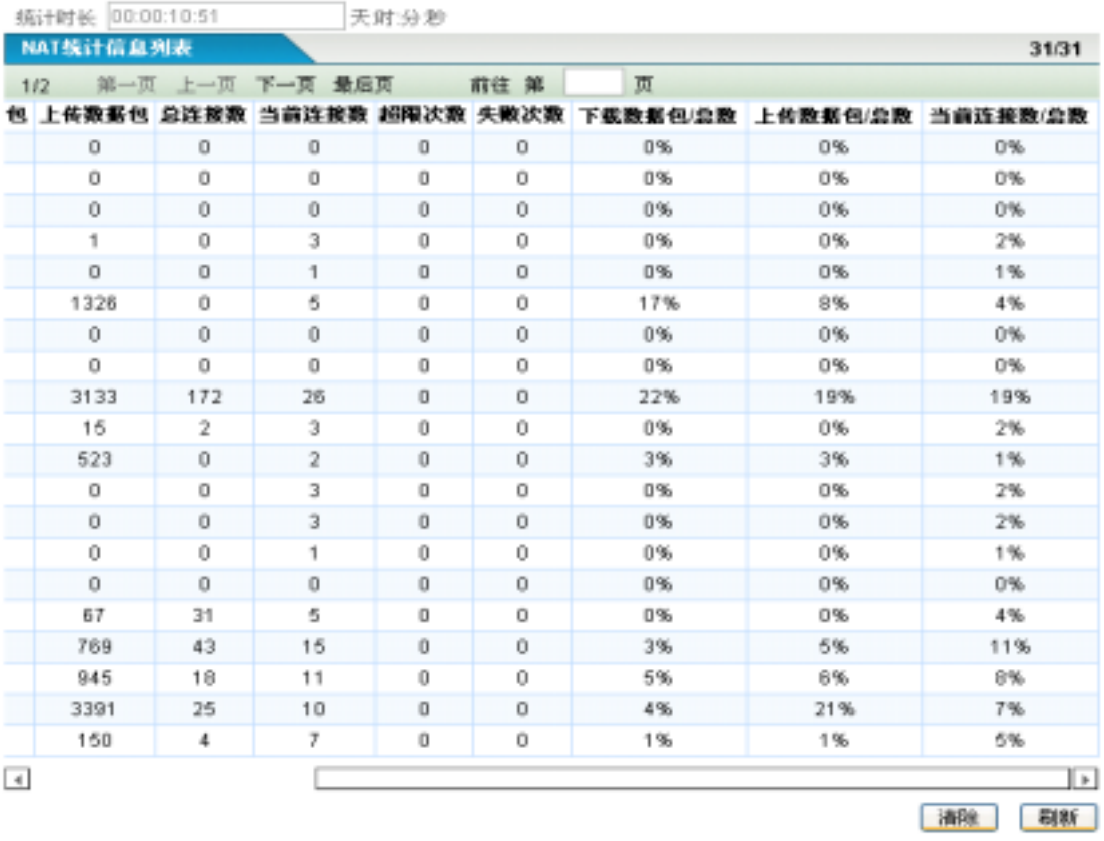
NAT统计信息列表 31/31

1/2 第一页 上一页 下一页 最后页 前往 第 页

ID	IP地址	活动记录	下载数据包	上传数据包	总连接数	当前连接数	超限次数	失败次数	下载数据包
1	0.0.0.0	xxxxxxxx	0	0	0	0	0	0	0%
2	172.168.16.5	0:04:48:40	0	0	0	0	0	0	0%
3	10.10.10.10	0:04:48:15	0	0	0	0	0	0	0%
4	200.200.200.15	0:00:04:48	0	1	0	3	0	0	0%
5	200.200.200.50	0:06:32:28	0	0	0	1	0	0	0%
6	200.200.200.54	0:00:00:00	2445	1326	0	5	0	0	17%
7	200.200.200.104	0:01:14:11	0	0	0	0	0	0	0%
8	200.200.200.109	0:03:52:50	0	0	0	0	0	0	0%
9	200.200.200.131	0:00:00:01	3255	3133	172	26	0	0	22%
10	200.200.200.150	0:00:00:55	6	15	2	3	0	0	0%
11	222.64.22.159	0:00:00:25	459	523	0	2	0	0	3%
12	200.200.200.168	0:00:47:53	0	0	0	3	0	0	0%
13	200.200.200.175	0:05:01:36	0	0	0	3	0	0	0%
14	200.200.200.178	0:01:55:54	0	0	0	1	0	0	0%
15	200.200.200.182	0:04:15:31	0	0	0	0	0	0	0%
16	200.200.200.183	0:00:00:25	58	67	31	5	0	0	0%
17	200.200.200.202	0:00:00:00	469	769	43	15	0	0	3%
18	200.200.200.205	0:00:00:02	667	945	18	11	0	0	5%
19	200.200.200.206	0:00:00:01	620	3391	25	10	0	0	4%
20	200.200.200.208	0:00:00:07	118	150	4	7	0	0	1%

清除 刷新

表 7-3 NAT 统计信息列表



统计时长 00:00:10:51 天:时:分:秒

NAT统计信息列表 31/31

1/2 第一页 上一页 下一页 最后页 前往 第 页

包	上传数据包	总连接数	当前连接数	超限次数	失败次数	下载数据包/总数	上传数据包/总数	当前连接数/总数
	0	0	0	0	0	0%	0%	0%
	0	0	0	0	0	0%	0%	0%
	0	0	0	0	0	0%	0%	0%
	1	0	3	0	0	0%	0%	2%
	0	0	1	0	0	0%	0%	1%
	1326	0	5	0	0	17%	8%	4%
	0	0	0	0	0	0%	0%	0%
	0	0	0	0	0	0%	0%	0%
	3133	172	26	0	0	22%	19%	19%
	15	2	3	0	0	0%	0%	2%
	523	0	2	0	0	3%	3%	1%
	0	0	3	0	0	0%	0%	2%
	0	0	3	0	0	0%	0%	2%
	0	0	1	0	0	0%	0%	1%
	0	0	0	0	0	0%	0%	0%
	67	31	5	0	0	0%	0%	4%
	769	43	15	0	0	3%	5%	11%
	945	18	11	0	0	5%	6%	8%
	3391	25	10	0	0	4%	21%	7%
	150	4	7	0	0	1%	1%	5%

清除 刷新

表 7-4 NAT 统计信息列表（续表 7-3）

- 统计时长：上一次清除至查询时刻的时间间隔，单位：天:时:分:秒；
- ID：序号；
- IP 地址：该用户的 IP 地址；
- 活动记录：该用户上一次使用 NAT 距离查询时刻的时间；
- 下载数据包：“ 统计时长 ” 内，该用户做 NAT 下载数据包的数量；
- 上传数据包：“ 统计时长 ” 内，该用户做 NAT 上传数据包的数量；
- 总连接数：“ 统计时长 ” 内，该用户使用的 NAT 会话的总数量；
- 当前连接数：该用户正在使用的 NAT 会话的数量；
- 超限次数：“ 统计时长 ” 内，该用户 NAT 请求超过 HiPER 内部限制的数量，用户最大 NAT Session 数在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置***（章节 6.3.2）中配置；
- 失败次数：“ 统计时长 ” 内，某用户 NAT 请求失败的数量；
- 下载数据包/总数：“ 统计时长 ” 内，该用户下载的数据包在整个局域网用户下载数据包总数中所占的百分比；
- 上传数据包/总数：“ 统计时长 ” 内，该用户上传的数据包在整个局域网用户上传数据包总数中所占的百分比；
- 当前连接数/总数：该用户实时的 NAT 会话数在 HiPER 当前 NAT 会话总数中所占的百分比；

- 清除：单击 “ 清除 ” 按钮，可清除 “ NAT 统计信息列表 ” 中的大部分信息，包括 “ 下载数据包 ”、“ 上传数据包 ”、“ 总连接数 ”、“ 超限次数 ”、“ 失败次数 ”、“ 下载数据包/总数 ”、“ 上传数据包/总数 ”。配合刷新按钮，可查看清除时刻至刷新时刻这段时间内的 NAT 统计信息。
- 刷新：单击 “ 刷新 ” 按钮，可以看到最新的 “ NAT 统计信息列表 ”。
- 排序：单击表中的某个参数，所有信息条目将按照该值的大小排序，方向为从小到大；再次单击该参数，排序方向将变为从大到小。例如，如果单击“ 当前连接数 ”，则表里的所有信息条目将按照“ 当前连接数 ”的值从小到大排序，如果再次单击“ 当前连接数 ”，排序方向将变为从大到小。

提示：

1. HiPER 的防攻击功能会限制用户 NAT 会话的总数量，当某用户 NAT 请求超过最大 NAT Session 数时，超过的连接将会被丢弃，并在 “ 超限次数 ” 中增加记录；同时通过查看 Syslog 服务的日志记录，可帮助管理员发现可能的 DoS 攻击；
2. 当系统资源不足（可能由于系统繁忙，或是遭受攻击引起）时，将会导致用户请求 NAT 失败，并在 “ 失败次数 ” 中增加记录；
3. 查询“ 统计时长 ”内，从 Internet 下载数据包最多的用户：上表“ 下载数据包/总数 ” 数值最大，例如表 7-3 中 ID 为 9 的用户；
4. 查询“ 统计时长 ”内，向 Internet 上传数据包最多的用户：上表“ 上传数据包/总数 ” 数值最大，例如表 7-3、7-4 中 ID 为 19 的用户；
5. 查询目前上网最活跃的用户：“ 当前连接数/总数 ” 数值最大，例如表 7-3、表 7－4 中 ID 为 9 的用户；
6. 查询 “ 统计时长 ” 内，可能使用端口扫描软件的用户：“ 超限次数 ” 大于 100，或是 “ 上传数据包 ” 数量远远大于 “ 下载数据包 ” 数量；
7. 查询 “ 统计时长 ” 内，可能使用 DoS/DDoS 攻击 HiPER 的用户：“ 上传数据包 ” 数量很大，“ 下载数据包 ” 数量很小或者没有。

7.3　端口统计

本节主要讲述 ***WEB 管理界面—>系统状态—>端口统计***的使用。

表 7-5 端口统计信息列表

表 7-6 端口统计信息列表（续表 7-5）

- ID：序号；
- 端口号：某端口，可以是物理端口或者是虚端口。In 代表从该端口进入 HiPER，Out 代表从该端口离开 HiPER；
- 字节数：上一次清除至查询时刻这段时间内，经过此端口的数据包字节数的统计；
- 数据包：上一次清除至查询时刻这段时间内，经过此端口的数据包数量的统计；
- 广播包：上一次清除至查询时刻这段时间内，经过此端口的广播包数量的统计，包括多播数据包的数量；
- 平均速率：上一次清除至查询时刻这段时间内，此端口接收或发送数据包的平均速率，给出每秒比特数（pps）和每秒数据包数（bps）两种表示方式。
- 入流量/出流量：上一次清除至查询时刻这段时间内，从该端口进入 HiPER 的数据包数量和从该端口离开 HiPER 的数据包的数量之百分比；
- 广播包/数据包：上一次清除至查询时刻这段时间内，经过此端口广播包数量和单播包数量之百分比；
- 丢弃包：上一次清除至查询时刻这段时间内，经过此端口的被丢弃包数量的统计。注意：HiPER 将把超过处理能力而来不及处理的数据包丢弃；
- 错误包：上一次清除至查询时刻这段时间内，经过此端口的错误包数量的统计；
- 未知包：上一次清除至查询时刻这段时间内，经过此端口的未知类型数据包数量

的统计；

- 非路由包：上一次清除至查询时刻这段时间内，经过此端口的非路由数据包（例如桥接、VLAN 发的包）数量的统计。
- 清除：单击“ 清除 ”按钮，可清除“ 端口统计信息列表 ”中的全部信息。配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的端口统计信息；
- 刷新：单击“ 刷新 ”按钮，可以看到最新的“ 端口统计信息列表 ”。

提示：一个正常的 HiPER 运行时应该具备的特征：

1. 广域网端口接收数据包数量与局域网端口发出数据包数量相近，广域网端口可能是一个或者两个（双线路接入）；
2. 广域网端口发出数据包数量与局域网端口接收数据包数量相近，广域网端口可能是一个或者两个（双线路接入）；
3. 广域网端口接收数据包的字节数与局域网端口发出数据包字节数相近，广域网端口可能是一个或者两个（双线路接入）；
4. 广域网端口发出数据包的字节数与局域网端口接收数据包的字节数相近，广域网端口可能是一个或者两个（双线路接入）；
5. 每个端口的“ 广播包/数据包 ”的百分比小于 5%；
6. 整个网络流量比较平衡，流量缓增缓减，不会出现瞬间流量突增的情况。

7.4　路由和端口信息

本节主要讲述 ***WEB 管理界面—>系统状态—>路由和端口信息***的使用。

7.4.1 路由表信息

路由器（网关）的主要工作就是为经过路由器的每个数据包寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表，供路由选择时使用。路由表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

路由表信息列表　　18/18

1/2　第一页　上一页　下一页　最后页　前往 第 [ ] 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	36
127.0.0.0/8	-	bhole0	cup	20	0	0	12732
127.0.0.1/32	-	local	cuhp	20	0	0	12732
127.0.0.2/32	-	reject0	cuhp	20	0	0	12732
127.0.0.3/32	-	bhole0	cuhp	20	0	0	12732
172.16.11.0/24	192.168.18.254	ie2	lugpa	60	1	0	36
192.168.16.0/24	-	ie0	cua	20	0	2039	12732
192.168.16.101/32	-	local	cuhp	20	0	638	12732
192.168.18.0/24	-	ie2	cua	20	0	3	12732
192.168.18.1/32	-	local	cuhp	20	0	0	12732

刷新

表 7-7 路由表信息列表

表 7-8 路由表信息列表（续表 7-7）

- 目的地址：目的网段的 IP 地址；
- 网关地址：到目的网段的网关 IP 地址；
- 端口号：符合该路由的数据包将从指定端口转发。
  ie0：物理接口 LAN；ie1：物理接口 WAN；ie2：物理接口 DMZ/WAN2；
  ptpdial0：待拨的虚端口；ptpx：虚端口 x；
  bhole0：内部接口，转发到该端口的所有包都被 HiPER 丢弃；
  local：内部软路由接口，转发到 HiPER 本身；
  reject：内部接口，转发到该端口的所有数据包都被 HiPER 拒绝，并回应一个 ICMP 不可达；
  loopback：回环地址，代表 127.0.0.0/8 网段，不被转发；
  mcast：多播；
- 路由状态：*–Hidden，o–OSPF，i–ICMP，l–Local，r–RIP，n–SNMP， c–Connected，s–Static，R–Remote，g–Gateway，h–Host，p–Private，u–Up，t–Temp，M –Multiple，N–NAT，F–Float，a–Append，?-Unknown；
  *-Hidden：此条路由目前不生效，一般是此条路由处于备份状态或是线路失效导致路由中断；
  N–NAT：此条路由上启用了 NAT，局域网用户正通过此条路由共享上网；
  F–Float：此条路由配置了路由优先级等信息，目前处于浮动状态，会因为线路的生效或者失效而决定该条路由是否启用。
- 优先级：该路由的优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的路由转发数据包，值越低优先级越高；
- 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1，优先级相同情况下，优先选择跳数值较低的路由；
- 使用次数：该路由被使用的次数；
- 使用时间：该路由生成的年龄（单位：秒）。
- 刷新：单击“ 刷新 ”按钮，可以在“ 路由表信息列表 ”看到最新相关信息。

下面以表 7-13、表 7-14 为例，对一些路由信息进行解释：

- 0.0.0.0/0——缺省路由：当一个数据包的目的网段不在路由记录中，那么，HiPER 将把该数据包发送到缺省路由的网关。缺省路由的网关是由配置的静态网关或者

PPPoE 拨号所得 IP 地址决定的；

- 127.0.0.0/8——本地环路：127.0.0.0 这个网段内所有地址都指向 HiPER 本身，如果收到这样一个数据包，应该发向 HiPER 本身；
- 172.16.11.0/24——指定网段的路由记录：当 HiPER 收到发往指定网段的数据包时，会将数据包发送到该条路由指定的网关（192.168.18.254）；
- 192.168.16.101/32——本地主机路由：当 HiPER 收到发送给自己的数据包时会将该数据包收下，并且不再转发；
- 224.0.0.0/4——组播路由：HiPER 收到一个组播数据包时，以组播的形式发送；
- 255.255.255.255/32——广播路由：当 HiPER 收到一个链路层广播包时将该数据包发送到 ie0。

在双线路接入的时候会看到两条缺省路由信息：

1. 负载均衡时的缺省路由信息（以两条固定 IP 接入为例），如表 7-9 所示。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第 [ ] 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	61.12.150.21	ie2	lugpamNF	60	1	0	17
0.0.0.0/0	200.200.200.254	ie1	lugpamNF	60	1	0	127

表 7-9 路由表信息列表——实例一

2. 负载均衡时的一条线路中断时的缺省路由信息（以两条固定 IP 接入为例），中断的线路路由状态前有标记“ * ”，如表 7-10 所示。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第 [ ] 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	8
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	120	1	0	45

表 7-10 路由表信息列表——实例二

3. 线路备份时的缺省路由信息（以两条固定 IP 接入为例），备份线路的路由状态前有标记“ * ”，如表 7-11 所示。

路由表信息列表　19/19

1/2　第一页　上一页　下一页　最后页　前往 第 [ ] 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaNF	60	1	0	20
0.0.0.0/0	61.12.150.21	ie2	*lugpaNF	61	1	0	20

表 7-11 路由表信息列表——实例三

7.4.2 端口信息

端口信息列表

1/1　第一页　上一页　下一页　最后页　前往 第　页

端口所在的接口	端口状态	速率状态	工作状态	模式状态
eth1	UP	100M	Full	MDI-X
eth1	UP	100M	Full	MDI
eth1	UP	100M	Full	MDI
eth1	DOWN	-	-	-
eth2	UP	10M	Half	MDI-X
eth3	DOWN	-	-	-

刷新

表 7-12 端口信息列表

- 端口所在的接口：该端口所在的物理接口。
  eth1：物理接口 LAN（交换口 1~交换口 4）；
  eth2：物理接口 WAN；
  eth3：物理接口 DMZ/WAN2；
- 端口状态：该端口是否激活。
  UP：激活；
  DOWN：未激活；
- 速率状态：该端口的连接速率；
  100M：协商结果为 100M 连接；
  10M：协商结果为 10M 连接；
- 工作状态：该端口的工作状态；
  Half：半双工；
  Full：全双工；
- 模式状态：该端口的工作模式；
  MDI：正接；
  MDI-X：反接；

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的“ 端口信息列表 ”。

提示：MDI 是指通过收发器发送的 100BASE-T 信号，即 100BASE-TX、FX、T4 或 T2 信号。将集线器连接网络接口卡时，其发送和接收对通常是相互连接的。集线器之间连接时，通常需要一条跨接电缆，其中的发送和接收对是反接的。MDI 是正常的 UTP 或 STP 连接，而 MDI-X 连接器的发送和接收对是在内部反接的，这就使得不同的设备（如集线器-集线器或集线器-交换机），可以利用常规的 UTP 或 STP 电缆实现背靠背的级联。

7.5　系统信息

本节讲述 ***WEB 管理界面—>系统状态—>系统信息***的使用，主要包括系统版本、系统运行时间、系统历史记录等信息。

7.5.1 系统版本

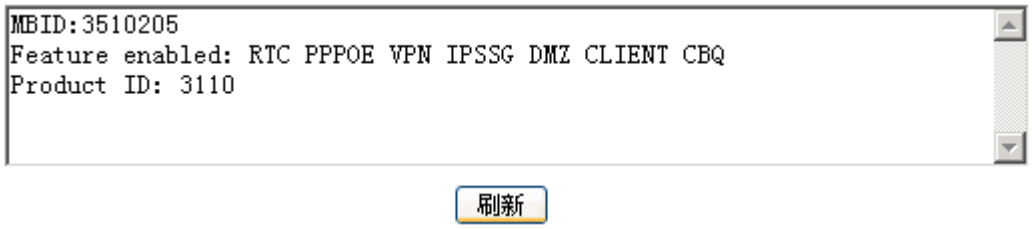


图 7-1 系统版本信息

版本信息	信息含义
MBID: 3510205	产品内部序列号（和机器表面序列号可能不同）
Feature enabled: RTC PPPOE VPN IPSSG DMZ CLIENT CBQ	产品具有的功能模块
Product ID: 3300NB	产品的型号

表 7-13 系统版本信息描述

7.5.2 系统运行时间

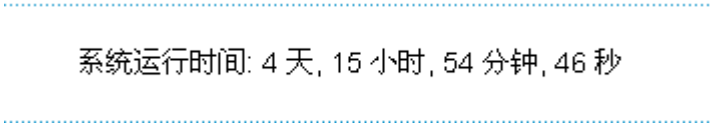


图 7-2 系统运行时间

7.5.3 系统历史记录

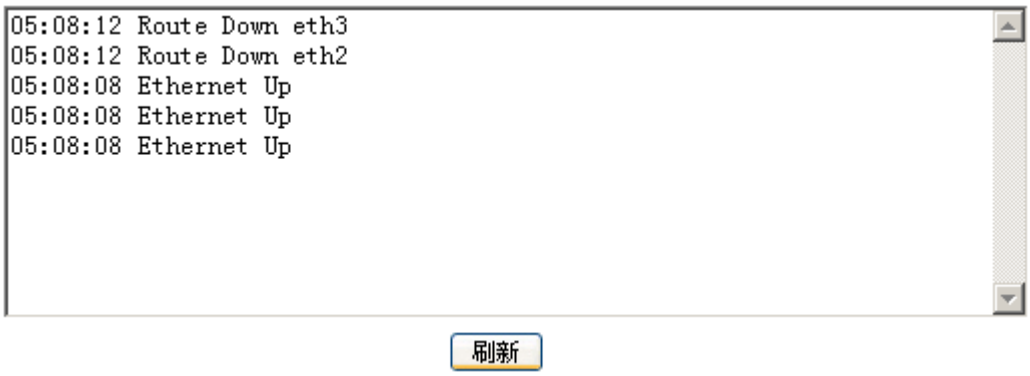


图 7-3 系统历史记录

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的系统历史记录。

提示：

1. 系统历史记录中，信息按照从旧到新的顺序从下往上排列；
2. 系统会显示最近十五条系统历史记录，记录的含义如表 7-14 所示：

历史记录	记录含义
Ethernet Up	某个物理接口被激活
MAC New 00:22:aa:00:22:bb MAC Old 00:22:aa:00:22:aa MAC Chged 192.168.16.221	该用户变化后的 MAC 地址 该用户变化前的 MAC 地址 连接到 HiPER 的 IP 地址为 192.168.16.221 的用户的 MAC 地址发生变化
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @61:1-1	某连接成功建立，[x]为连接名 PPPoE 成功和 MAC 地址为 00:0c:f8:f9:66:c6 的设备建立连接 物理层/链路层连接完成，但 IP 仍不可用 连接开始呼出
Call Terminated @clearSession: 1 Outgoing Call @61:1-1	呼叫失败 连接开始呼出
Session down [x]	某连接挂断，[x]为连接名
Session up [x] Assigned to port Call Connected, on Line1, on Channel0 Incoming Call	某连接成功建立，[x]为连接名 协商成功，为拨入的连接分配端口 物理层/链路层连接完成，但 IP 仍不可用 有远端呼叫拨入
Security error [x]	安全层错误

NAT exceeded 192.168.16.221	表示该 IP 地址的计算机 NAT 并发 session 超过了系统限定的最大 session 数（在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置***〈章节 6.3.2〉中配置）。一般情况下是这台计算机感染了病毒或者是在进行黑客攻击，如果一切正常，请适当调高最大 session 数这个参数。
Route Up ethX： Route Down ethX：	该物理端口上配置的路由生效（一般是该端口物理线路启用所致） 该物理端口上配置的路由中断（一般是该端口物理线路中断所致）

表 7-14 系统历史记录

7.6　系统异常信息

本节讲述 ***WEB 管理界面—>系统状态—>系统异常信息***的使用，如图 7-4 所示。

图 7-4 系统异常信息

- 刷新：单击“ 刷新 ”按钮，可以看到最新的系统异常信息。
- 提示：如果 HiPER 在运行过程中，发生了一些错误，系统会在这里生成一条记录，在寻求艾泰科技工程师支持的时候，请提供这些错误记录。

第8章　上网监控

本章主要讲述如何监控局域网用户上网状况。在 HiPER 中，可以根据全部记录、主线路、备份线路、内网地址、外网地址/域名、外网端口以及 NAT 地址/域名等条件查询内网用户上网情况。此时查询的是局域网用户当前使用 NAT 的信息，并不是 NAT 统计信息。

当内网中有主机向外发出连接请求时，HiPER 将会在 NAT 表中为该请求建立一条 NAT Session（NAT 会话）的记录，从而将该主机内部的 IP 地址转化为合法的 IP 地址进行通信。这种由内到外、或者由外向内的连接就是一个 NAT Session。

8.1　查询条件

图 8-1 选择查询条件

- 选择查询的条件：
  全部记录——查询当前全部用户的上网信息；
  主线路——查询使用主线路上网的局域网用户的上网信息；
  备份线路——查询使用备份线路上网的局域网用户的上网信息 ;只有配置了备份线路，才可以选择此项进行查询；
  内网地址——填写局域网用户的 IP 地址，查询该用户此时的上网信息；
  外网地址/域名——填写 Internet 地址或者网站的域名，查询当前局域网用户到此地址的连接信息；
  外网端口——填写目的端口，查询局域网用户此时使用某种 Internet 上网业务的信息（常用协议端口号：TCP21：ftp；TCP22：ssh；TCP23：telnet；TCP25：smtp；UDP53：dns；TCP79：finger；TCP80：http；TCP110：pop3；UDP161：snmp）；
  NAT 地址/域名——填写局域网用户上网使用的 IP 地址，使用多地址 NAT 时，可以查询正在使用该 IP 地址上网的局域网用户的上网信息；
- 查询参数：根据选择的查询条件，输入相应的查询参数；
- 常用端口选择：当选择查询条件为“ 外网端口 ”时，这里可以查询常用的业务端口。
- 查询：单击“ 查询 ”按钮，即可按条件查询。
- 提示：

1. 只有系统管理员才有上网监控权限，在 ***WEB 管理界面—>系统管理—>管理员配置***（章节 5.1）中可查看和配置管理员权限；
2. 只有配置了备份线路，才能查询使用备份线路上网的局域网用户的上网信息；
3. 本章所提及的“ 主线路 ”、“ 备份线路 ”分别对应“ 主线路 NAT 规则 ”及“ 备份线

路 NAT 规则 ”，主线路（备份线路）NAT 规则是配置线路时系统自动生成的 NAT 规则，具体描述详见 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 功能介绍***（章节 6.3.1）。

8.2　上网监控查询页面

查询结果列表　　125/125

1/7　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.15	69	U	0.0.0.0	0	0	0	218.80.175.179	69
2	200.200.200.15	23	T	0.0.0.0	0	0	0	222.64.21.23	2023
3	200.200.200.15	123	U	192.5.41.209	ntp	1	0	222.64.21.23	6202
4	200.200.200.50	6333	T	211.144.97.11	38915	30	27	222.64.21.23	6333
5	200.200.200.50	3389	T	0.0.0.0	0	0	0	222.64.21.23	3389
6	200.200.200.50	5631	T	0.0.0.0	0	0	0	222.64.21.23	5631
7	200.200.200.50	5632	U	0.0.0.0	0	0	0	222.64.21.23	5632
8	200.200.200.54	14895	T	202.96.211.53	pptp	27	14	222.64.21.23	6426
9	200.200.200.54	123	U	131.107.1.10	ntp	5	3	222.64.21.23	6241
10	200.200.200.54	0	G	202.96.211.53	0	277	0	222.64.21.23	3666
11	200.200.200.54	53764	I	10.0.1.14	3114	51	0	222.64.21.23	3114
12	200.200.200.104	0	I	202.96.209.5	7538	6	0	222.64.21.23	7538
13	200.200.200.104	1354	T	200.255.253.241	53	11	10	222.64.21.23	7511
14	200.200.200.104	1355	T	200.255.253.241	53	12	10	222.64.21.23	7509
15	200.200.200.104	1353	T	200.255.253.241	53	14	10	222.64.21.23	7507
16	200.200.200.114	3030	T	207.46.107.3	msn	53	39	222.64.21.23	6987
17	200.200.200.114	3375	T	207.46.107.163	msn	0	0	222.64.21.23	6986
18	200.200.200.114	3396	T	207.46.108.52	msn	0	0	222.64.21.23	6968
19	200.200.200.131	1449	T	211.157.106.59	http	5	5	218.80.175.179	7561
20	200.200.200.131	1439	U	221.236.11.14	qq	47	45	222.64.21.23	7490

表 8-1 查询结果列表

- ID：序号；
- 内网地址：该 NAT 会话的源地址；
- 内网端口：该 NAT 会话使用的源端口；
- 协议类型：该 NAT 会话使用的协议类型（T：TCP；U：UDP；I：ICMP）或协议号；
- 外网地址：该 NAT 会话要访问的目的地址；
- 外网端口：该 NAT 会话的目的端口。系统预设了一些标准业务，如 dns 解析、ftp 下载、www 浏览、smtp 发信、pop3 收信、qq、msn、qiji2（奇迹 2）、cq（传奇）、cs（cs 游戏）等；
- 上传数据包：该 NAT 会话上传数据包的数量；
- 下载数据包：该 NAT 会话下载数据包的数量；
- NAT 地址：该 NAT 会话经过 NAT 转换后的 IP 地址；
- NAT 端口：该 NAT 会话经过 NAT 转换后使用的端口；

8.3　查询实例

8.3.1 查询局域网 IP 地址为 200.200.200.198/24 的用户当前上网行为

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-2 所示；
第二步，在“ 选择查询条件 ”中选择“ 内网地址 ”；
第三步，在“ 查询参数 ”中填入 200.200.200.198；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-2 所示。

图 8-2 选择查询条件——实例一

查询结果列表　　6/6

1/1　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.198	3013	U	202.96.199.133	dns	7	0	218.80.175.179	7522
2	200.200.200.198	3020	U	219.133.40.74	qq	11	11	222.64.21.23	3651
3	200.200.200.198	3008	T	207.46.106.87	msn	127	103	222.64.21.23	3647
4	200.200.200.198	3012	U	202.96.170.164	qq	57	206	222.64.21.23	3642
5	200.200.200.198	3027	T	218.21.71.104	telnt	27	34	222.64.21.23	3456
6	200.200.200.198	3011	T	207.68.178.238	http	7	6	222.64.21.23	3057

表 8-2 查询结果列表——实例一

8.3.2 查询局域网内目前访问 www.utt.com.cn 的用户

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-3 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网地址/域名 ”；
第三步，在“ 查询参数 ”中填入 www.utt.com.cn；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-3 所示。

图 8-3 选择查询条件——实例二

查询结果列表　　7/7

1/1　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.114	3029	T	61.152.95.143	http	123	190	222.64.21.23	6990
2	200.200.200.114	3053	T	61.152.95.143	http	776	1174	222.64.21.23	6909
3	200.200.200.114	3066	T	61.152.95.143	http	65	86	218.80.175.179	6829
4	200.200.200.174	1067	T	61.152.95.143	http	30	29	222.64.21.23	7553
5	200.200.200.174	1066	T	61.152.95.143	http	18	24	218.80.175.179	6641
6	200.200.200.206	1685	T	61.152.95.143	http	16	18	218.80.175.179	5840
7	200.200.200.206	1686	T	61.152.95.143	http	21	20	222.64.21.23	4703

表 8-3 查询结果列表——实例二

8.3.3 查询局域网内目前使用 MSN 的用户

第一步，进入 ***WEB 管理界面—>上网监控***页面，如图 8-4 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网端口 ”；
第三步，在“ 查询参数 ”中填入 1863；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-4 所示。

图 8-4 选择查询条件——实例三

查询结果列表　　35/35

1/2　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.114	3030	T	207.46.107.3	msn	156	109	222.64.21.23	6987
2	200.200.200.114	3375	T	207.46.107.163	msn	0	0	222.64.21.23	6986
3	200.200.200.114	3396	T	207.46.108.52	msn	0	0	222.64.21.23	6968
4	200.200.200.114	3062	T	207.46.108.5	msn	334	527	222.64.21.23	6948
5	200.200.200.114	3057	T	207.46.108.48	msn	88	85	222.64.21.23	6921
6	200.200.200.131	1410	T	207.46.108.62	msn	4	4	222.64.21.23	7332

表 8-4 查询结果列表——实例三

8.3.4 查询局域网内目前使用 WAN2 口 IP 地址上网的信息

提示：如果使用双线路上网，可在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息***（章节 4.1.1）中，查询备份线路连接信息中的“ IP 地址 ”，即可得到 WAN2/DMZ 口的 IP 地址。

第一步，进入 ***WEB 管理界面—>上网监控***页面，如图 8-5 所示；
第二步，在“ 选择查询条件 ”中选择“ NAT 地址/域名 ”；
第三步，在“ 查询参数 ”中填入 218.80.175.179（本例中，当前 WAN2 口地址为

218.80.175.179）；

第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-5 所示。

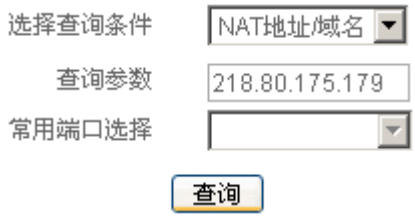


图 8-5 选择查询条件——实例四

查询结果列表　31/31

1/2　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.15	69	U	0.0.0.0	0	0	0	218.80.175.179	69
2	200.200.200.131	1504	U	202.96.199.133	dns	7	0	218.80.175.179	7487
3	200.200.200.131	1505	U	202.96.199.133	dns	2	1	218.80.175.179	5897
4	200.200.200.150	2906	U	202.96.199.133	dns	10	2	218.80.175.179	3621
5	200.200.200.174	1054	T	207.46.106.120	msn	102	129	218.80.175.179	7559
6	200.200.200.174	1122	T	220.194.61.196	http	10	6	218.80.175.179	6634

表 8-5 查询结果列表——实例四

8.3.5 查询局域网内目前使用主线路上网的信息

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-6 所示；

图 8-6 查询条件——实例五

第二步，在“ 选择查询条件 ”中选择“ 主线路 ”；

第三步，单击“ 查询 ”按钮，即可查询，查询结果如表 8-6 所示。

查询结果列表　97/97

1/5　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.15	23	T	0.0.0.0	0	0	0	222.64.21.23	2023
2	200.200.200.15	123	U	192.5.41.209	ntp	3	1	222.64.21.23	6202
3	200.200.200.50	6333	T	211.144.97.11	41469	193	178	222.64.21.23	6333
4	200.200.200.50	3389	T	0.0.0.0	0	0	0	222.64.21.23	3389
5	200.200.200.50	5631	T	0.0.0.0	0	0	0	222.64.21.23	5631
6	200.200.200.50	5632	U	0.0.0.0	0	0	0	222.64.21.23	5632
7	200.200.200.54	0	I	10.6.35.10	7326	6	0	222.64.21.23	7326
8	200.200.200.54	14895	T	202.96.211.53	pptp	97	55	222.64.21.23	6426

表 8-6 查询结果列表——实例五

8.3.6 查询局域网内目前使用备份线路上网的信息

第一步，进入 ***WEB 管理界面***—>***上网监控***页面，如图 8-7 所示；

图 8-7 查询条件——实例六

第二步，在“选择查询条件”中选择“备份线路”；

第三步，单击“查询”按钮，即可查询，查询结果如表 8-7 所示。

查询结果列表　　21/21

1/2　第一页　上一页　下一页　最后页　前往 第　页

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.15	69	U	0.0.0.0	0	0	0	218.80.175.179	69
2	200.200.200.174	1054	T	207.46.106.120	msn	122	147	218.80.175.179	7559
3	200.200.200.199	3225	T	61.187.99.9	http	6	5	218.80.175.179	7789
4	200.200.200.199	3224	T	61.187.99.9	http	35	25	218.80.175.179	7788
5	200.200.200.199	3218	T	61.187.99.9	http	20	13	218.80.175.179	7782
6	200.200.200.200	4546	T	159.226.40.150	ftpdt	3	1	218.80.175.179	7810
7	200.200.200.201	4000	U	202.104.129.254	qq	58	65	218.80.175.179	5939
8	200.200.200.201	1343	T	207.46.108.85	msn	11	14	218.80.175.179	5051

表 8-7 查询结果列表——实例六

第9章　带宽业务

通过带宽业务管理功能，可将 ISP 分配的带宽二次分配给各工作组。针对各工作组不同的上网要求，分配不同大小的带宽并设定不同的优先级。这样，上网要求高的工作组不仅可以获得较高的带宽，还可以获得较大的优先级，从而保证其用户在网络繁忙时可以优先上网，避免因为带宽不足影响应用（比如视频会议等）的有效运行。

同时，还可以通过“ 平均分配本类带宽给组内用户 ”，避免组内某用户占用过多带宽，导致影响组内其他用户正常上网。HiPER 还支持不同工作组之间带宽共享，避免空闲带宽浪费。通过“ 允许借用其他组空闲带宽 ”，实现本组业务繁忙带宽不足时可以借用其他组空闲带宽 ；通过“ 允许本组带宽空闲时外借 ”，实现其他组业务繁忙时可以借用本组空闲带宽。

提示：使用带宽业务管理功能时，必须禁止快速转发（在 ***WEB 管理界面—>高级配置—>特殊功能—>快速转发***〈章节 6.6.1〉中配置）；如果需要带宽业务管理，推荐启用内网主机速率限制功能（在 ***WEB 管理界面—>高级配置—>特殊功能—>内网主机速率限制***〈章节 6.6.2〉中配置）。

9.1　带宽管理基本信息配置

图 9-1 带宽管理基本信息配置

- 物理接口带宽 :LAN 物理接口实际最大发送速率，可选 10Mbps 连接或者 100Mbps 连接（可以通过接口 100Mbps 指示灯辨别）；
- ISP 分配带宽：ISP 分配给用户的实际带宽。很多情况下，运营商给用户分配的实际带宽要小于其标称带宽，这里必须知道线路的实际可用带宽；
- 保存：带宽配置参数生效；
- 取消：恢复旧的配置参数数据。
- 提示：

1. 单位换算 1Mbps=1024Kbps，1Kbyte=8Kbps；
2. 物理接口带宽和 ISP 分配带宽填写不准确会造成带宽管理不能按照预想设置工作。

9.2　带宽管理策略配置

图 9-2 带宽管理策略配置

- 剩余带宽：当前剩余的带宽，由系统自动生成。剩余带宽加上以前配置的带宽之和就是总带宽；
- 组选择 :选择要定义带宽的工作组(已在 ***WEB 管理界面—>高级配置—>组管理***〈章节 6.1〉中定义)，选定工作组后，这一行的右边会显示该组的用户 IP 地址段；
- 分配带宽：填写为该组用户分配的实际带宽；
- 优先级：优先级由高到低依次为高——次高——中——低，当配置了优先级后，当 HiPER 繁忙的时候会优先处理优先级高的工作组的数据；
- 允许借用其他组空闲带宽：选中，本组用户可以使用其他工作组空闲的带宽，这样就可避免因其他组带宽空闲时造成浪费带宽的现象；
- 允许本组带宽空闲时外借：选中，其他工作组可以使用本组的空闲带宽，这样就可避免因本组带宽空闲时造成浪费带宽的现象；
- 平均分配本类带宽给组内用户：选中，平均分配本组带宽给组内各在线用户。这样就可避免同组内用户相互争用带宽的现象。
- 保存：带宽配置参数生效；
- 重填：恢复到修改前的配置参数。
- 提示：

1. 当物理接口带宽或 ISP 分配带宽发生变化时，原有的带宽分配策略全部失效，这时候需要重新配置带宽分配策略；
2. 各组分配带宽之和不能超过 ISP 分配带宽；
3. 系统会自动生成一个带宽策略，将没有分配的剩余带宽分配给没有配置带宽策略的其他用户；
4. 目前带宽业务管理功能在 NAT 环境下只能实现对下行（下载）带宽的管理。

9.3 带宽业务列表

表 9-1 带宽业务列表

- 增加带宽业务：选中“ 添加 ”选项，输入带宽业务信息，单击“ 保存 ”按钮，生成新的带宽业务；
- 浏览带宽业务：如果已经生成了带宽业务，可以查看“ 带宽业务列表 ”(如表 9-1)，浏览带宽业务相关信息；
- 编辑带宽业务：如果想编辑某一带宽业务，只需单击此带宽业务后面的“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除带宽业务：选中一些带宽业务，单击右下角的“ 删除 ”按钮，即可删除被选中的带宽业务。

9.4　自定义带宽业务

第一步，进入 ***WEB 管理界面—>带宽业务***页面；

第二步，根据实际情况，输入局域网物理带宽和实际 ISP 分配带宽，单击“ 保存 ”按钮；

第三步，为每个工作组规划上网带宽和优先级；

第四步，选中“ 添加 ”选项，选择该带宽业务要匹配的工作组（在 ***WEB 管理界面—>高级配置→组管理***〈章节 6.1〉中定义）；

第五步，根据规划输入为该组分配的带宽大小；

第六步，根据规划设置该组带宽的优先级；

第七步，根据规划设置该组带宽的是否可以外借，是否可以借用，是否需要平均分配；

第八步，单击“ 保存 ”按钮，该带宽业务配置成功，可以在“ 带宽业务列表 ”中看到相应的记录；

第九步，继续配置其他工作组的带宽业务；

第十步，所有工作组带宽配置完成后，如有剩余带宽，系统会自动生成一个带宽策略，将没有分配的带宽分配给没有配置带宽的其他用户。

提示：若要删除带宽业务，只需在“ 带宽业务列表 ”中选中要删除的带宽业务，单击“ 删除 ”按钮即可。

9.5　带宽业务配置实例

1.　应用需求

公司背景同 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***（章节 6.1.4）

中
的实例。该公司的管理部门、技术部门、销售部门通过共享 2Mbps ADSL 线路上网，公司局域网物理接口带宽为 100Mbps。

该公司希望通过分别给这 3 个不同的部门分配不同大小的带宽并设定不同的优先级，以保证整个公司的数据通讯不会受到某个突发的数据流的影响。

各部门 IP 地址、带宽分配如表 9-2 所示，该表中，“ 允许借入 ”指“ 允许借用其他组空闲带宽 ”、“ 允许借出 ”指“ 允许本组带宽空闲时外借 ”、“ 平均分配 ”指“ 平均分配本类带宽给组内用户 ”。

部门	组名	IP 地址范围	分配带宽	优先级	允许借入	允许借出	平均分配
销售部	Sale	192.168.16.50~ 192.168.16.70	512Kbps	中		√	
技术部	Technique	192.168.16.120~ 192.168.16.150	1024Kbps	次高	√		√
管理部	Admin	192.168.16.160~ 192.168.16.180	256Kbps	高	√		
其他	Other	本方案中其他空闲的 IP 地址	256Kbps		√	√	

表 9-2 带宽业务配置信息

2. 分析

由表 9-2，可以看出，在本方案中，销售部门（工作组 Sale）共获得 512Kbps 带宽，优
先级为中，同时允许该组带宽空闲时外借。技术部门（工作组 Technique）共获得 1024Kbps 带宽，优先级为次高，同时由于该部门各员工上网业务要求相当，故设置该组用户平均该类分配带宽，同时允许该组用户借用其他组空闲带宽。管理部门（工作组 Admin）共获得 256Kbps 带宽，优先级设为高，同时允许该组用户借用其他组空闲带宽。公司的其他部门获得剩余的 256Kbps 带宽。

3. 配置步骤

第一步，进入 ***WEB 管理界面—>带宽业务***页面；

第二步，在“ 物理接口带宽 ”选择中“ 100M ”，在“ ISP 分配带宽 ”中填入 2048，如图 9-1 所示，单击“ 保存 ”按钮；

第三步，如表 9-2 所示，为各工作组规划上网带宽和优先级；

第四步，配置工作组 Sale 带宽业务。

如图 9-2 所示，选中“ 添加 ”选项，在“ 组选择 ”中选择“ Sale ”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***〈章节 6.1.4〉中定义），在“ 分配带宽 ”中填入 512，“ 优先级 ”选择“ 中 ”，选中“ 允许本组带宽空闲时外借 ”选项，单击“ 保存 ”按钮，工作组 Sale 带宽业务配置完成，系统“ 剩余带宽 ”自动变为 1536Kbps；

第五步，配置工作组 Technique 带宽业务。

如图 9-3 所示，选中“ 添加 ”选项，在“ 组选择 ”中选择“ Technique ”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***〈章节 6.1.4〉中定义），在“ 分配带宽 ”中填入 1024，“ 优先级 ”选择“ 次高 ”，选中“ 允许借用其他组空闲带宽 ”选项和“ 平均分配本类带宽给组内用户“ 选项 ”，单击“ 保存 ”按钮，工作组 Technique 带宽业务配置完成，

系统“剩余带宽”自动变为 512Kbps；

图 9-3 带宽管理策略配置（Technique）

第六步，配置工作组 Admin 带宽业务。

如图 9-4 所示，选中“添加”选项，在“组选择”中选择“Admin”（已在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置实例***〈章节 6.1.4〉中定义），在“分配带宽”中填入 256，“优先级”选择“高”，选中“允许借用其他组空闲带宽”选项，单击“保存”按钮，工作组 Admin 带宽业务配置完成，系统“剩余带宽”自动变为 256Kbps；

图 9-4 带宽管理策略配置（Admin）

第七步，至此，三个工作组带宽配置完成，还有剩余带宽 256K，如图 9-5 所示，系统会自动生成一个带宽策略，将没有分配的剩余带宽分配给没有配置带宽策略的其他用户；

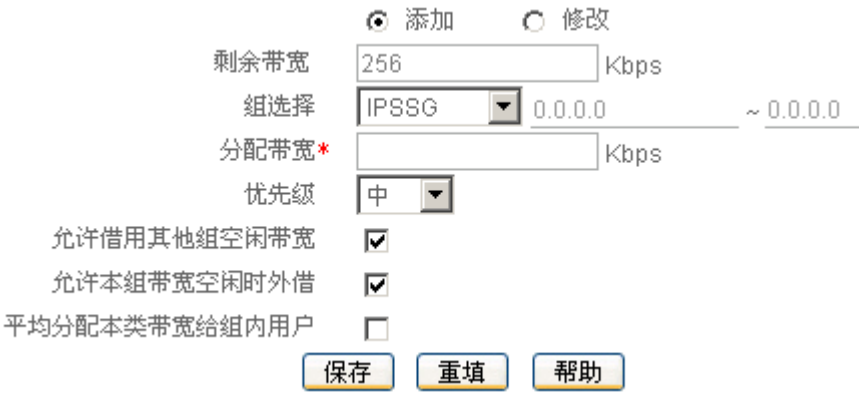


图 9-5 带宽管理策略配置(Other)

提示：删除带宽业务，在“带宽业务列表”中选中要删除的带宽业务，单击“删除按钮，即可删除被选中的带宽业务。

附录 A　配置局域网中的计算机

HiPER 配置完成之后，必须配置局域网中的计算机的 TCP/IP 属性。本章讲述如何在 Windows95/98 环境下配置计算机的 TCP/IP 属性。

第一步 检查网络 IP 状态

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，在“已经安装了下列网络组件”中查看是否已安装网卡的驱动程序与 TCP/IP 协议，如图 A-1 所示，如果出现了“TCP/IP->网卡型号”选项，就表示已经安装：

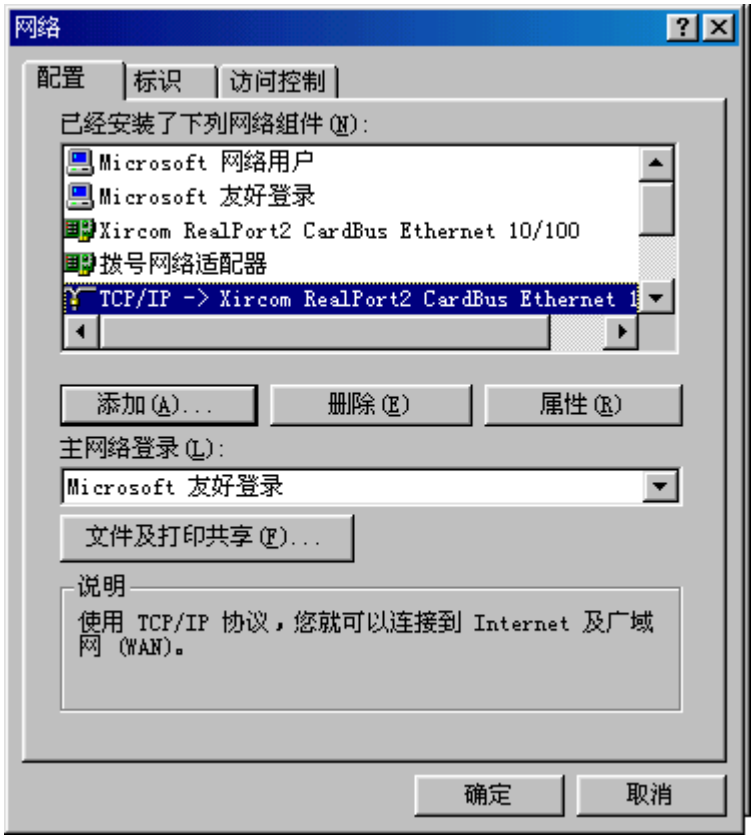


图 A-1 网络配置窗口

3. 如果没有安装网卡驱动程序及 TCP/IP 协议，首先需查阅网卡的原厂文件来安装匹配的网卡驱动程序。
4. 在安装网卡驱动程序之后，需添加 TCP/IP 传输协议。首先打开“网 络”窗口（步骤同前），如图 A-1 所示，再单击“添加”按钮，随后单击“协议”→“添加”→“Microsoft”→“TCP/IP 传输协议”即可。在指定的网卡完成添加 TCP/IP 协议后，需重启计算机来更新系统的网络设定，使其生效。

第二步 配置 TCP/IP 属性

下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

方法一 手工设置 IP 地址

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，如图 A-1 所示，在“已经安装了下列网络组件” 选择“TCP/IP->网卡型号”选项，再单击“属性”按钮；
3. 单击“IP 地址”菜单进入“IP 地址”配置窗口，如图 A-2 所示，首先选中“指定 IP 地址(S)”选项，然后在“IP 地址(I)”中填入：192.168.16.X（X 在 2 至 254 之间），在“子网掩码(U)”中填入 255.255.255.0；

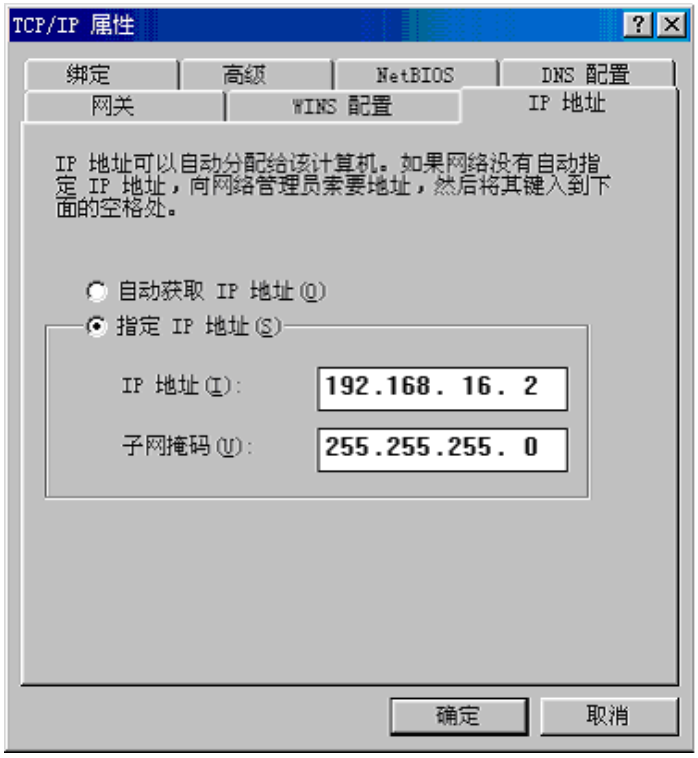


图 A-2 TCP/IP 属性 IP 地址配置窗口

4. 单击“网关”菜单进入“网关”配置窗口，如图 A-3 所示，首先在“新网关”选项中，填入 HiPER 的 LAN 口 IP 地址（出厂时为 192.168.16.1），然后单击“添加”按钮，新网关添加成功；

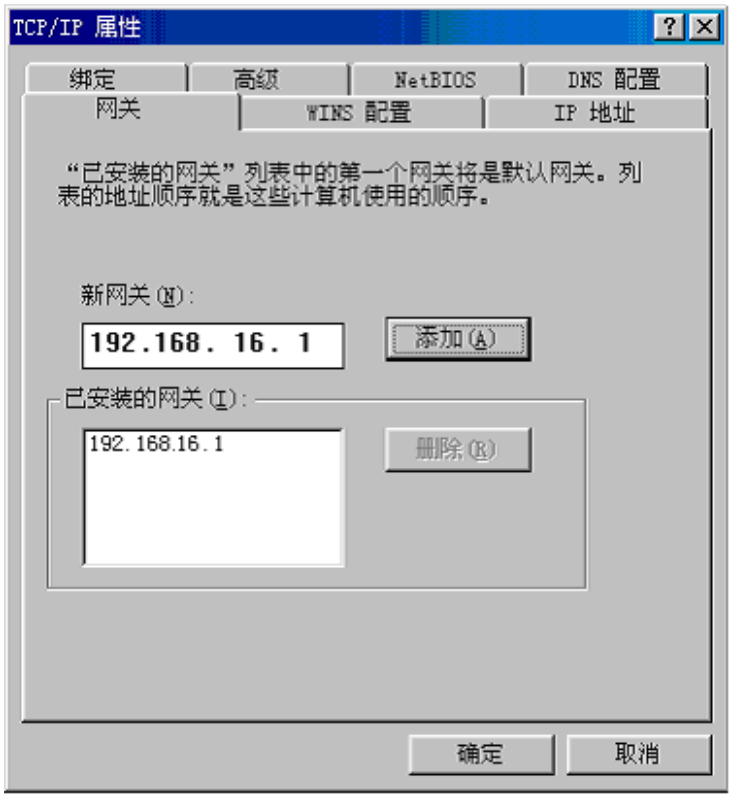


图 A-3 TCP/IP 属性网关配置窗口

5. 单击“ DNS 配置 ”菜单进入“ DNS 配置“ 窗口， 如图 A-4 所示，首先在“ 主机(H)”和“ 域(O) ”中任意填入主机名和域名，然后在“ DNS 服务搜索顺序 ”中填入 ISP 所提供的 DNS 服务器的 IP 地址（可向 ISP 询问），单击“ 添加 ”按钮，DNS 配置成功；

图 A-4 TCP/IP 属性 DNS 配置窗口

6. 以上配置完成后，单击“ 确定 ”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

方法二 通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在 HiPER 的 ***WEB 管理界面—>基本配置—>DHCP 和 DNS 服务器—>DHCP 服务配置***（章节 4.3.1）中激活 DHCP Server 功能；
2. 单击“ 开始 ”→“ 设置 ”→“ 控制面板 ”；
3. 双击“ 网络（network）”图标，单击“ 配置 ”菜单进入“ 配置 ”窗口，如图 A-1 所示，在“ 已经安装了下列网络组件 ” 选择“ TCP/IP->网卡型号 ”选项，再单击“ 属性 ”按钮；
4. 单击“ IP 地址 ”菜单进入“ IP 地址 ”配置窗口，如图 A-5 所示，选中“ 自动获取 IP 地址(O) ”；

图 A-5 TCP/IP 属性 IP 地址配置窗口

5. 单击“ 网关 ”菜单进入“ 网关 ”配置窗口，如图 A-6 所示,在“ 新网关 ”中不用填入任何值（如果原先有设置，请删除）；

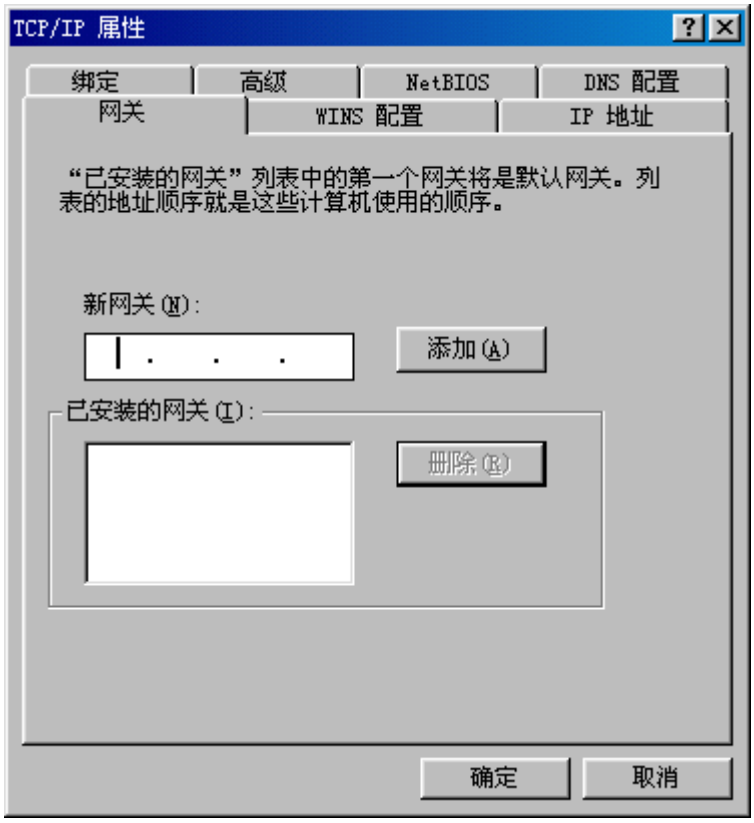


图 A-6 TCP/IP 属性网关配置窗口

6. 单击“ DNS 配置 ”菜单进入“ DNS 配置 “ 窗口， 如图 A-7 所示，在 DNS 设置选项中选择“ 禁用 DNS ”；

图 A-7 TCP/IP 属性 DNS 配置窗口

7. 以上配置完成后，单击“ 确定 ”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

第三步 浏览器设定

1. 单击“ 开始 ”→“ 程序 ”→“ 附件 ”→“ 通讯 ”→“ Internet 连接向导 ”；
2. 选择“ 手动设置 Internet 连接或通过局域网（LAN）连接 ”，单击“ 下一步 ”按钮；
3. 选择“ 通过局域网（LAN）连接 ”，单击“ 下一步 ”按钮；
4. 清除“ 局域网 Internet 配置 ”中的所有选项，单击“ 下一步 ”按钮；
5. 在“ 想现在设置一个 Internet 邮件帐户吗？ ”中，选择“ 否 ”，单击“ 下一步 ”按钮；
6. 单击“ 完成 ”按钮，结束“ Internet 连接向导 ”配置；

至此，TCP/IP 属性全部配置完成，现在已经可以正常使用浏览器、FTP client 或者其他的 Internet 客户端程序。

附录 B　FAQ

1. ADSL 用户如何上网？

1) 首先，将 ADSL Modem 设置为桥模式（1483 桥模式）；
2) 确认 PPPoE 线路是标准拨号型的（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）；
3) 用网线将 HiPER 的 WAN 口与 ADSL Modem 相连，并将电话线连接到 ADSL Modem 的 Line 口；
4) 在 ***WEB 管理界面—>快速向导—>上网接入线路配置—>PPPoE 拨号上网配置***（章节 3.2.4.1）中，配置 PPPoE 的相关参数；
5) 如果是包月上网的用户，可以选择拨号类型为“ 自动拨号 ”。如果是非包月上网的用户，可以选择拨号类型为“ 按需拨号 ”或者“ 手动拨号 ”，并且可以输入空闲时间，以防止忘记断线而浪费上网时间；
6) 如果选择了“ 手动拨号 ”，可以在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息—>PPPoE 拨号接入时线路连接信息***（章节 4.1.1.1）中进行手动拨号；
7) 拨号成功后，在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息—>PPPoE 拨号接入时线路连接信息***（章节 4.1.1.1）中可以查看 PPPoE 拨号成功后的配置和状态信息（如图 B-1），比如“ 连接状态 ”（拨号成功后正常显示为“ 已连接 ”）、ISP 分配的“ IP 地址 ”、“ 使用时间 ”等信息。

图 B-1 PPPoE 拨号主线路连接信息

8) 在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.5.3）中，可以查看连接历史记录，如表 B-1 所示。

呼叫历史记录	呼叫结果
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	PPPoE 拨号成功。
Call Terminated @clearSession: 1 Outgoing Call @51:1-1	物理连接无法建立，请检查线路是否正常（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）。
Call Terminated @clearSession: 1 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	物理已经建立，但是验证失败，请在 ***WEB 管理界面—>基本配置—>ISP 配置—>PPPoE 拨号上网的配置***（章节 4.1.2.1）中检查 PPPoE 用户名、密码配置是否正确。如果配置正确，请将验证方式修改成 CHAP 或者 NONE（如图 B-2），并且重启 HiPER。

表 B-1 PPPoE 拨号历史记录

图 B-2 PPPoE 拨号配置（部分）

9) 在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息***（章节 7.5.1）中，可以查看 ISP 分配的 IP 地址（“网关地址”），以及“路由状态”（必须看到 N，N 代表 NAT 启用）等信息，如表 B-2 所示；

路由表信息列表 25/25

1/3 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	222.64.21.185	ptp7	IuaN	60	1	282312	3256

表 B-2 路由表信息列表——实例一

10) 按照本手册附录 A 所述内容配置局域网计算机。

2. 固定 IP 接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；
2) 用网线将 HiPER 的 WAN 口与 ISP 网络设备相连；
3) 在 ***WEB 管理界面—>快速向导—>上网接入方式配置—>固定 IP 接入配置***（章节 3.2.4.2）中，配置固定 IP 接入的相关参数；
4) 配置完成后，在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息***（章节 7.5.1）中，可以查看“路由状态”（必须看到 N，N 代表 NAT 启用）等信息，如表 B-3 所示；

路由表信息列表 17/17

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	2239

表 B-3 路由表信息列表——实例二

5) 按照本手册附录 A 所述内容配置局域网计算机。

3. 动态 IP（Cable Modem）接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；
2) 用网线将 HiPER 的 WAN 口与 ISP 网络设备相连；
3) 在 ***WEB 管理界面—>快速向导—>上网接入方式配置—>动态 IP 接入配置***（章节 3.2.4.3）中，配置动态 IP 接入的相关参数；

提示：某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会导致新的网络设备（这里指 HiPER）无法正常获 IP 地址，此时需要将 HiPER 的 WAN 口 MAC 地址设置成和原有网络设备的 MAC 地址相同。在 ***WEB 管理界面—>基本配置—>ISP 配置***（章节 4.1.2）中，选择“连接类型”为“动态 IP 接入”，配置“广域网端口 MAC 地址”，单击“保存”按钮，重启 HiPER 后配置生效；

4) 在 ***WEB 管理界面—>基本配置—>ISP 配置—>线路连接信息—>动态接入时线路连接信息***（章节 4.1.1.3）中，可以查看动态 IP 接入时线路的配置和状态信息（如图 B-3），比如“连接状态”（正常连接时显示为“已连接”）、ISP 分配的“IP 地址”、“剩余租用时间”等信息。

图 B-3 动态 IP 接入时主线路连接信息

5) 在 ***WEB 管理界面—>系统信息—>路由和端口信息—>路由表信息列表***（章节 7.5.1）中，可以查看 ISP 分配的 IP 地址（“网关地址”）、“路由状态”（必须看到 N，N 代表 NAT 启用）等信息，如表 B-4 所示；

路由表信息列表 17/17

1/2 第一页 上一页 下一页 最后页 前往 第 页

目的地址	网关地址	端口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.254	ie1	lugpaN	60	1	0	24

表 B-4 路由表信息列表——实例三

6) 按照本手册附录 A 所述内容配置局域网计算机。

4. 如何将 HiPER 恢复到出厂配置?

提示：下述方法将删除设备原来所有配置，请谨慎使用。

下面介绍将 HiPER 恢复到出厂配置的方法，按知道或忘记管理员密码分别说明。

情况一：知道管理员密码

正常情况下，可以在 ***WEB 管理界面—>系统管理—>配置管理—>恢复出厂配置***（章节 5.4.3）中，选择“恢复设备出厂配置”选项来恢复出厂值。

也可以通过“超级终端”来恢复设备的出厂配置（为了安全起见，HiPER 并没有设置 Reset 按钮），步骤如下：

1) 首先，将随机附带的配置线一端（RJ45 接头）接入 HiPER 的 TERMINAL 接口，另一端（DB9 接头）接入计算机的串口。
2) 单击“开始”→“程序”→“附件”→“通讯”→“超级终端”（如果没有安装这个工具，请选择“我的电脑”→“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”→“通讯”，然后安装这个程序）。
3) 如图 B-4 所示，在“名称”中填入“HiPER1”，单击“确定”按钮。

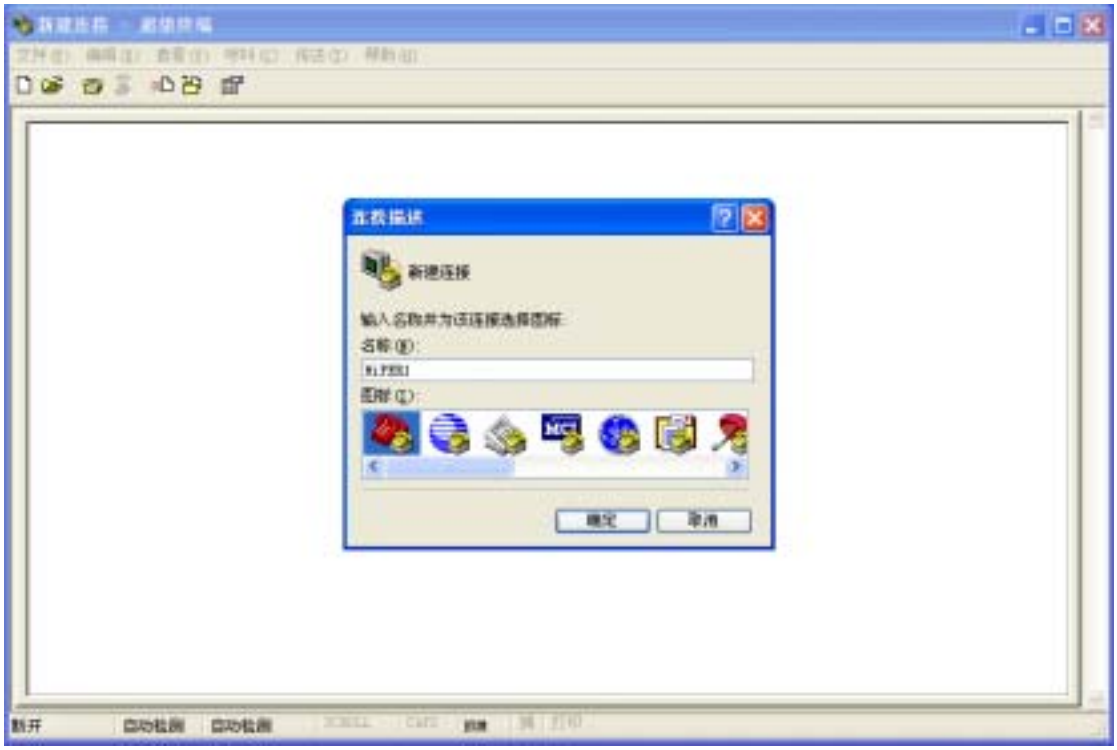


图 B-4 新建连接界面（9600）

4) 如图 B-5 所示，在“选择连接时使用”中选择 COM X（根据实际情况选择配置线实际

连接的计算机的串口），单击“ 确定 ”按钮。

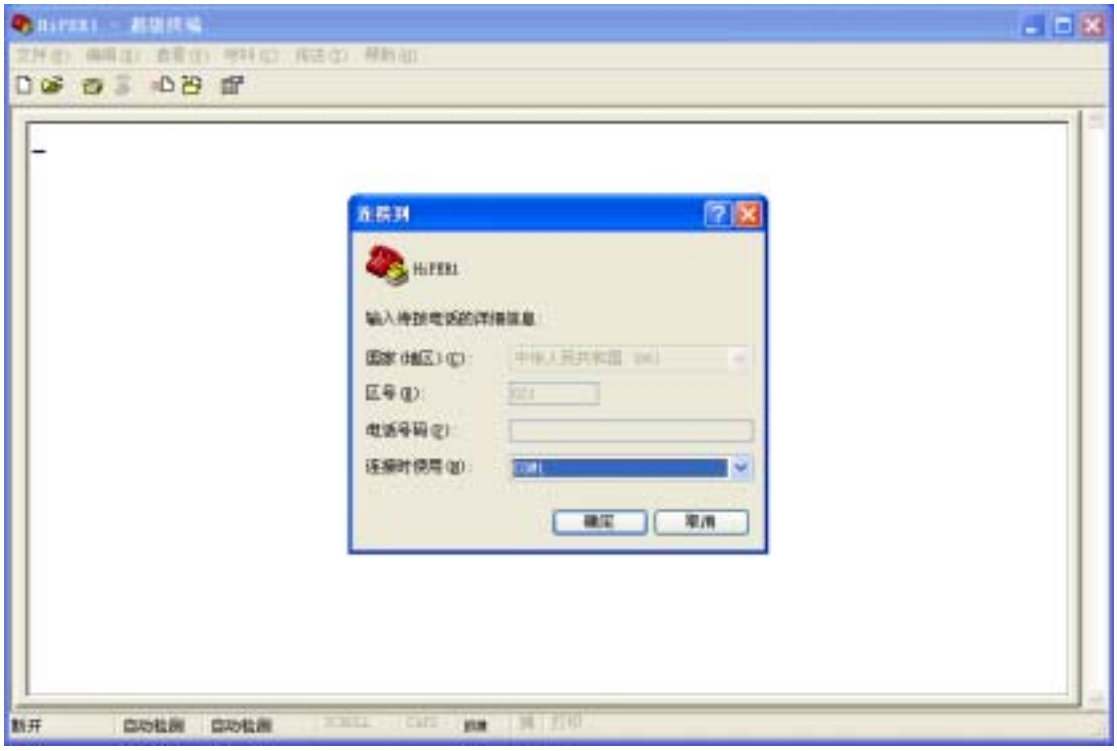


图 B-5 选择串口界面（9600）

5) 如图 B-6 所示，选择“ 每秒位数 ”：9600 ；“ 数据位 ”：8 ；“ 奇偶校验 ”：无 ；“ 终止位 ”：1 ；“ 数据流控制 ”：无，单击“ 确定 ”按钮。

图 B-6 COM 口属性配置界面（9600）

6) 进入如图 B-7 所示超级终端主控界面，输入<回车>。

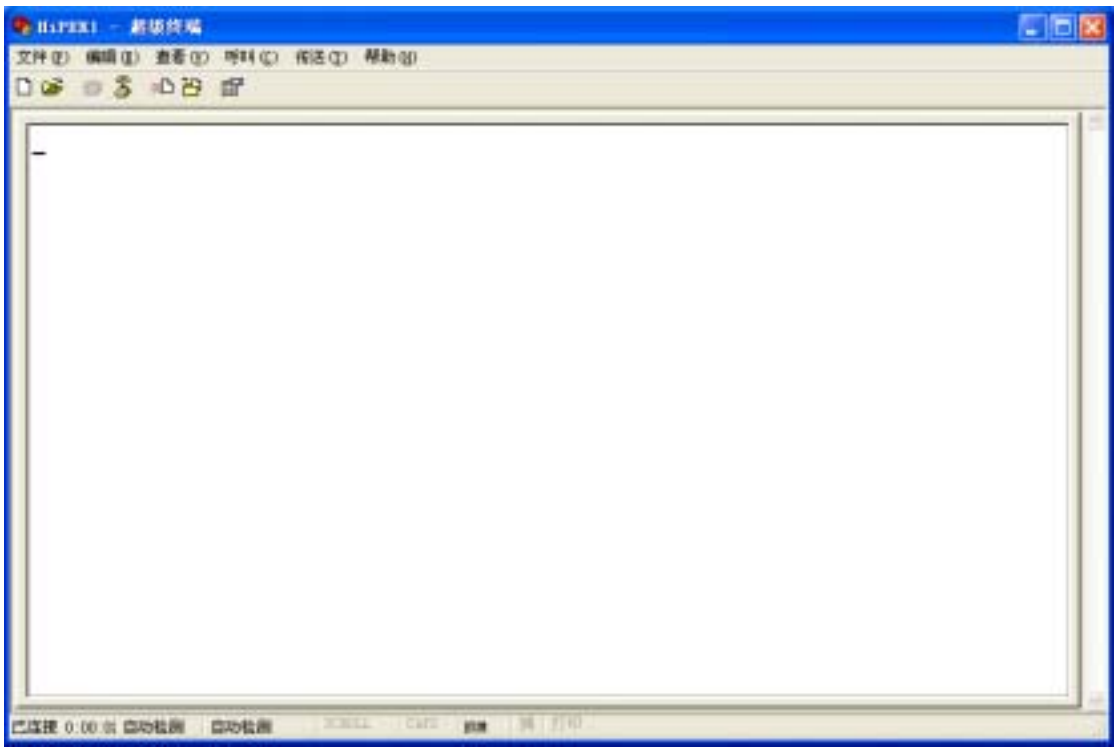


图 B-7 主控界面（9600）

7)　如图 B-8 所示，在“ Login：”后输入用户名<回车>（本例中用户名为 Default）。

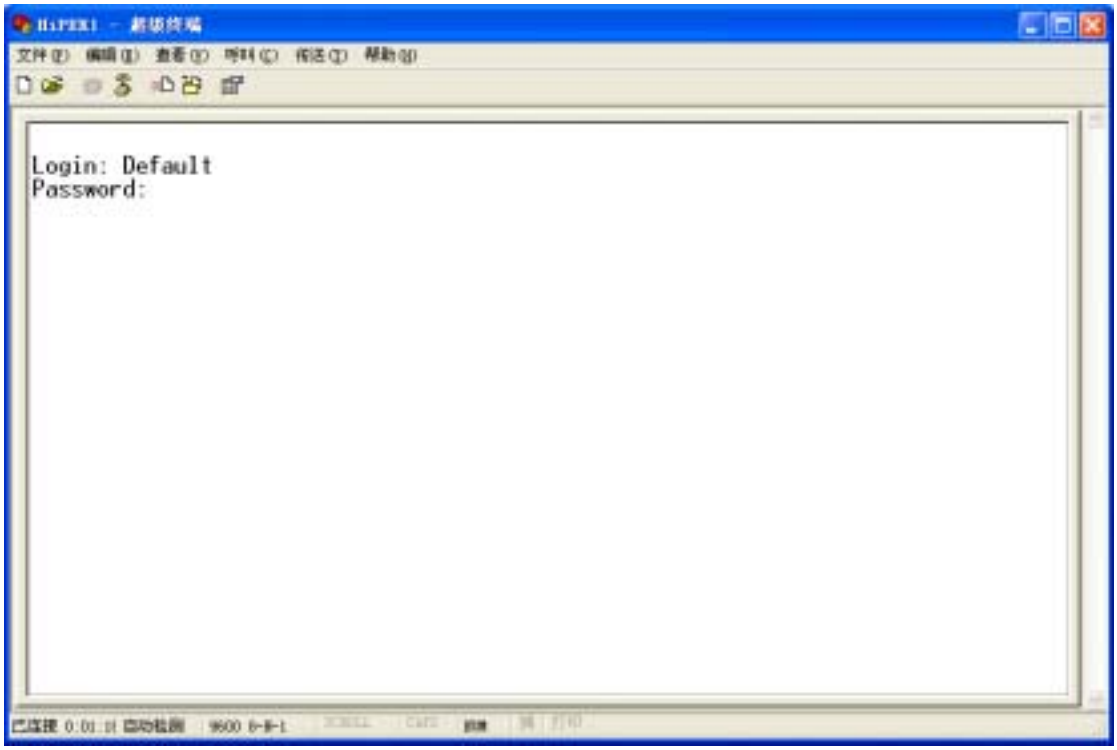


图 B-8 登录界面一（9600）

8)　如图 B-9 所示，在“ Password：”后输入密码<回车>（本例中密码为空）。

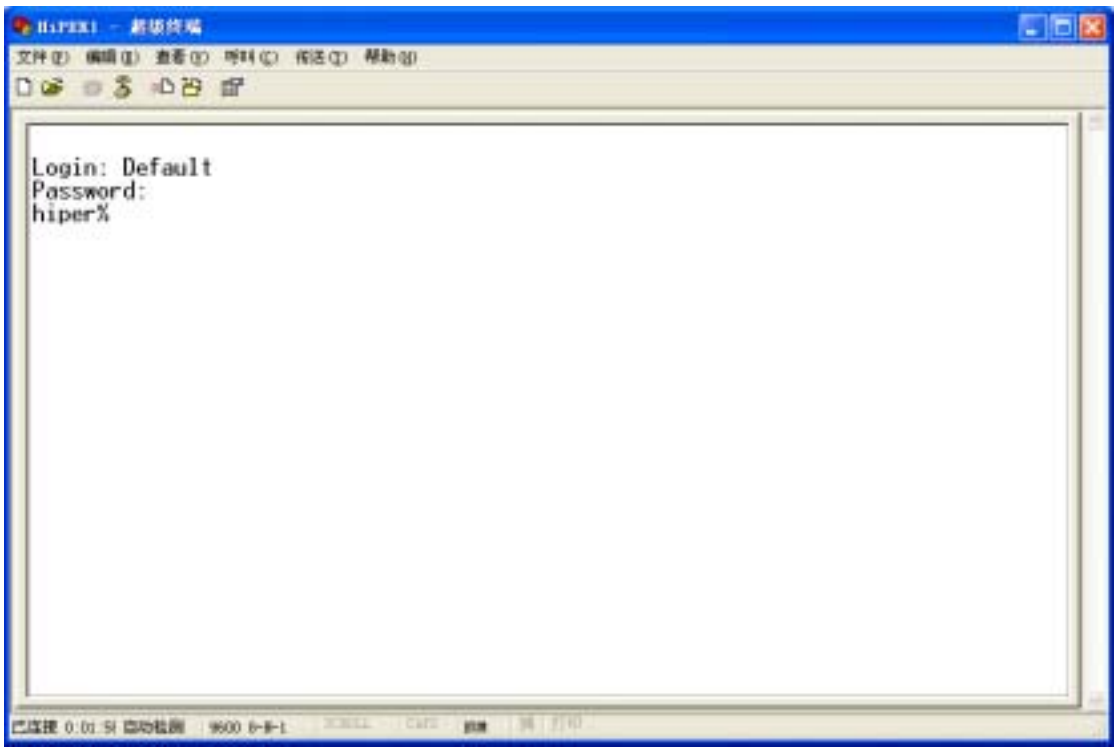


图 B-9 登录界面二（9600）

9) 如图 B-10 所示，输入 nvramc<回车>，HiPER 已经成功恢复出厂值。重启 HiPER 后，就可以通过局域网端口登录 WEB 管理界面（默认 IP 地址：192.168.16.1；用户名 Default；密码为空）。

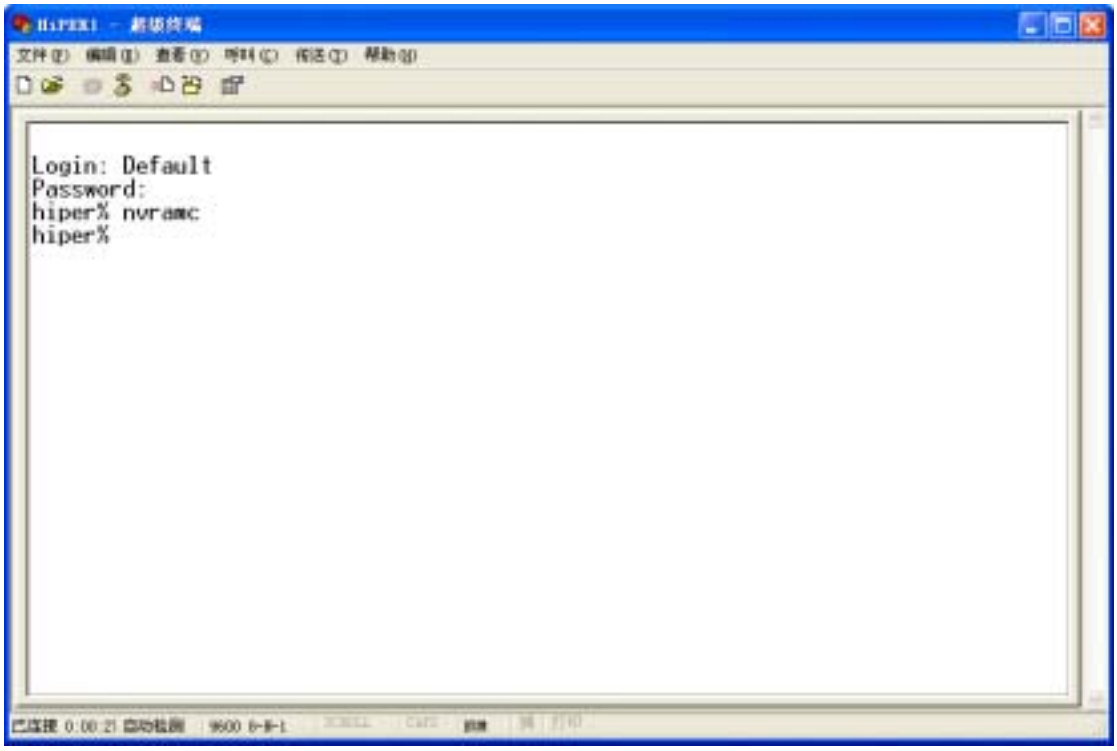


图 B-10 恢复出厂配置界面（9600）

情况二：忘记管理员密码

如果忘记了管理员口令的话，将无法进入 WEB 管理界面，此时只能通过“超级终端”来恢复设备的出厂配置（为了安全起见，HiPER 并没有设置 Reset 按钮）。

1) 首先，将随机附带的配置线一端（RJ45 接头）接入 HiPER 的 TERMINAL 接口，另一端（DB9 接头）接入计算机的串口。
2) 单击“开始”→“程序”→“附件”→“通讯”→“超级终端”（如果没有安装这个工具，请选择“我的电脑”→“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”→“通讯”，然后安装这个程序）。
3) 如图 B-11 所示，在“名称”中填入“HiPER2”，单击“确定”按钮。

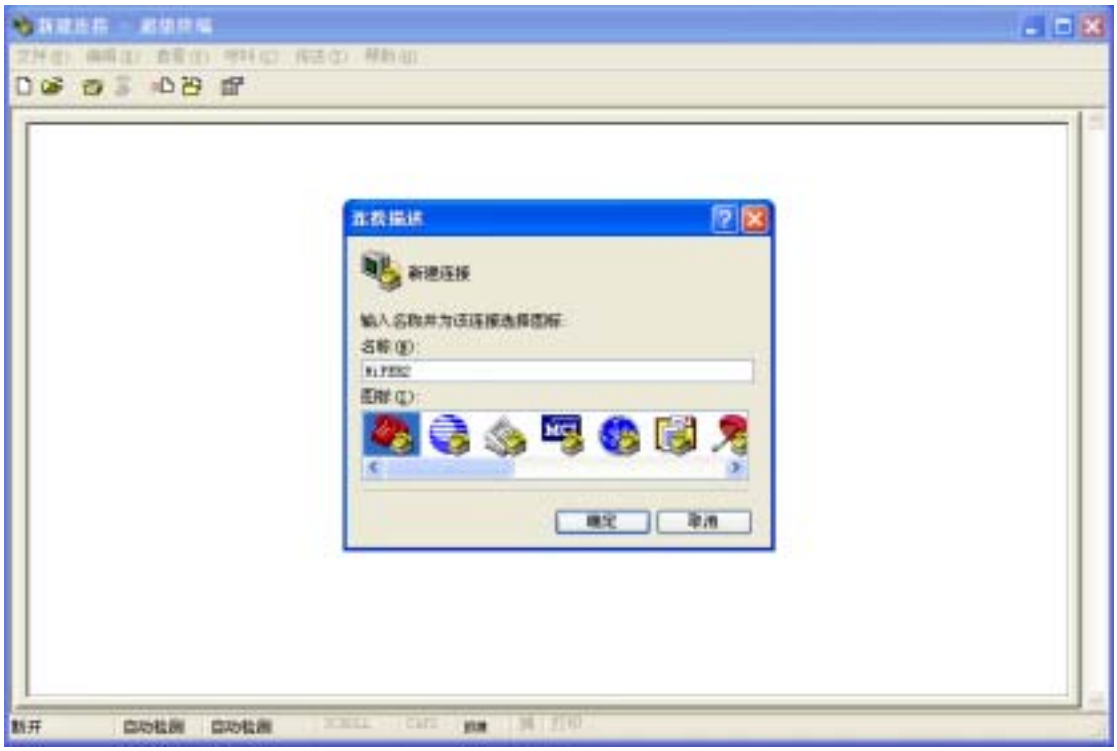


图 B-11 新建连接界面（115200）

4) 如图 B-12 所示，在“选择连接时使用”中选择 COM X（根据实际情况选择配置线实际连接的计算机的串口），单击“确定”按钮。

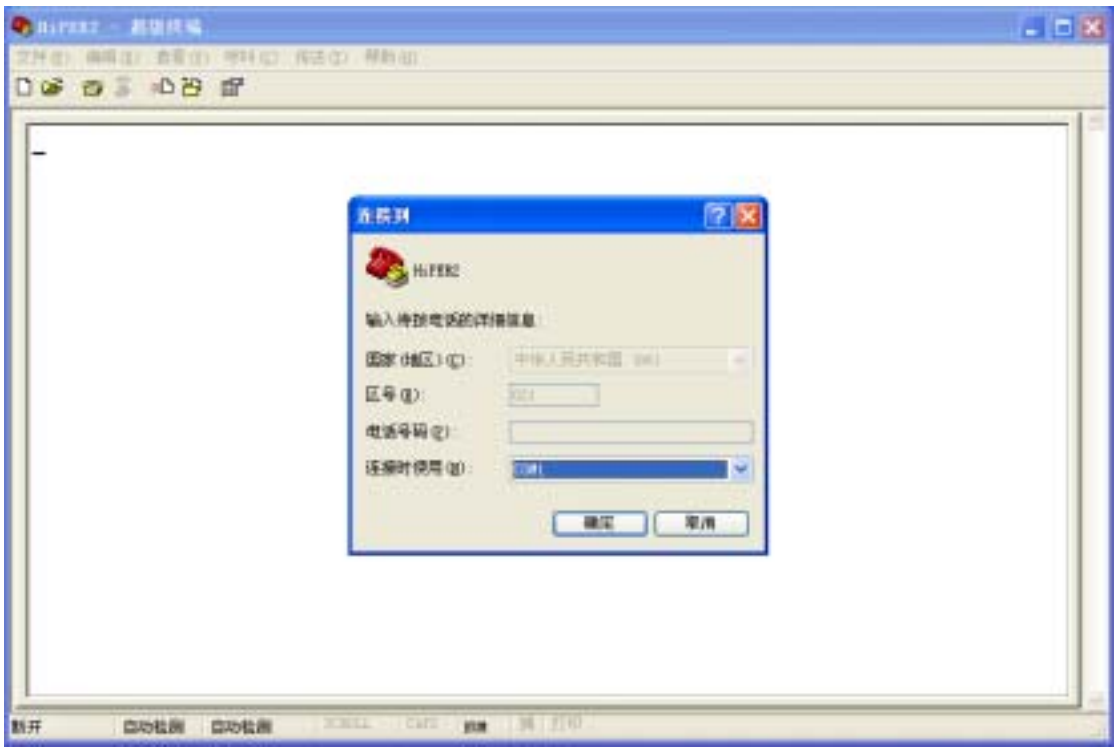


图 B-12 选择串口界面（115200）

5) 如图 B-13 所示，选择 “ 每秒位数 ”：115200 ；“ 数据位 ”：8 ；“ 奇偶校验 ”：无 ；“ 终止位 ”：1 ；“ 数据流控制 ”：无 ；单击 “ 确定 ” 按钮。

图 B-13 COM 口属性配置界面（115200）

6) 进入如图 B-14 所示超级终端主控页面。

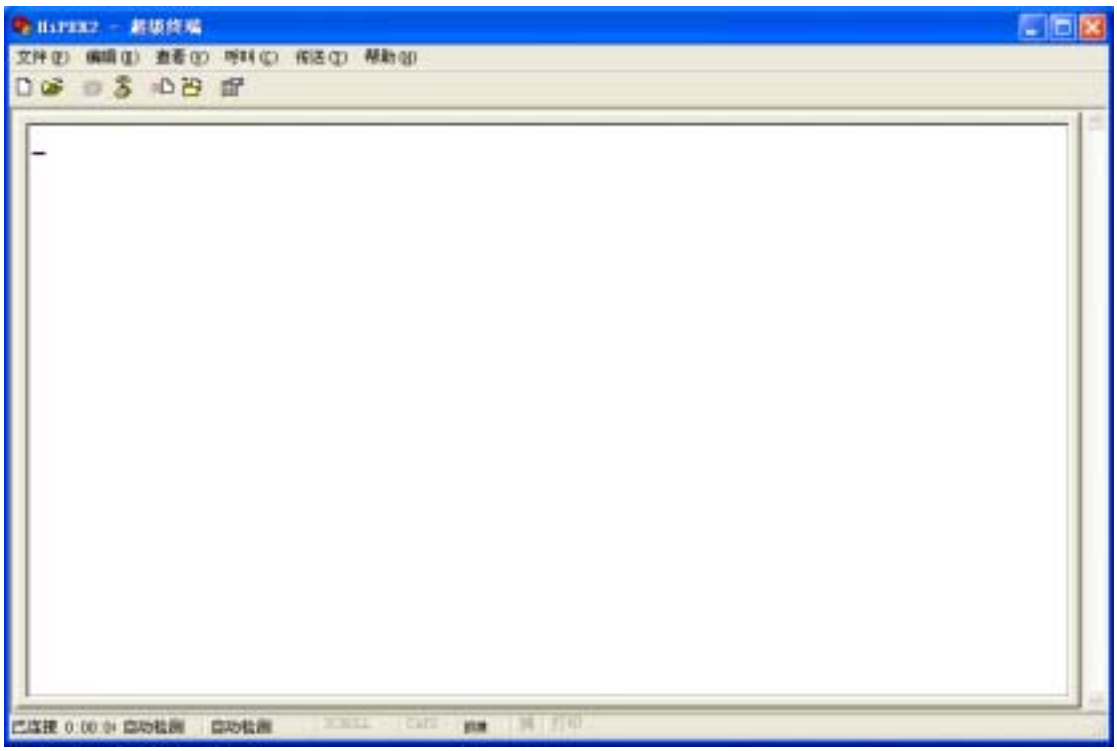


图 B-14 主控界面（115200）

7) 此时，重新启动 HiPER，在 3 秒钟之内顺序输入“ ast ”三个字母（全部小写），出现“ Ast> ”提示符（如不成功，可多试几次，直至出现该字符），如图 B-15 所示。

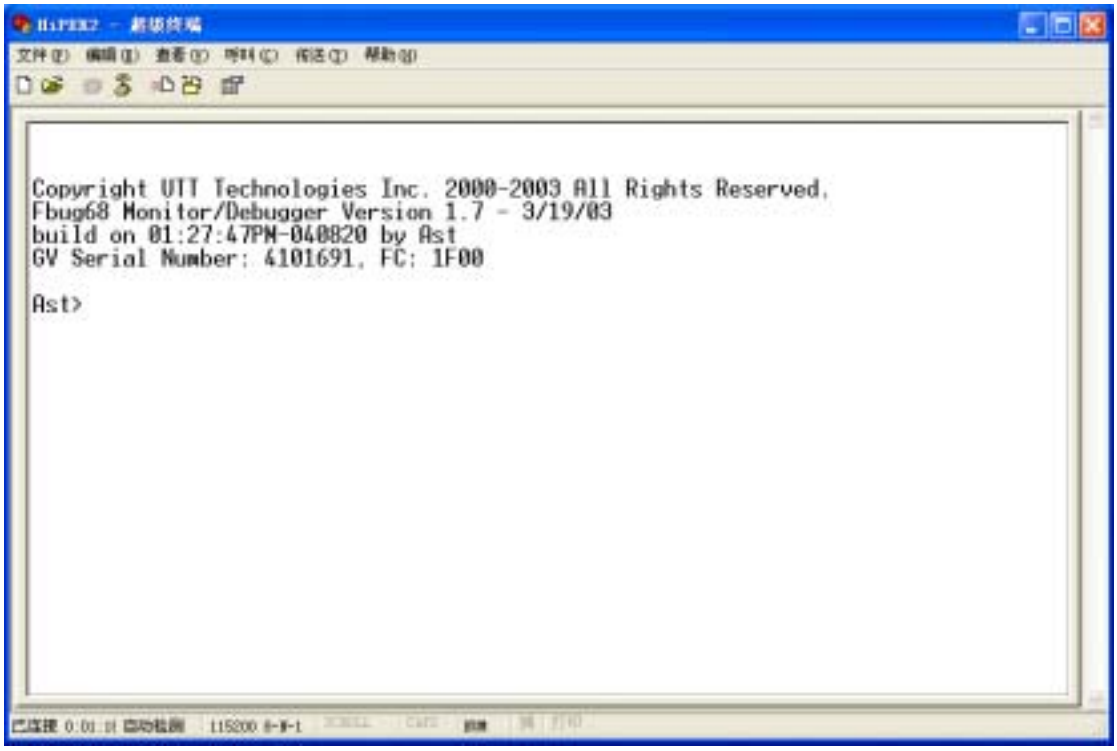


图 B-15 恢复出厂配置界面一（115200）

8) 恢复出厂配置

输入 nv<回车>，出现“ Erasing NVRAM……Done ”，如图 B-16 所示，代表 HiPER 已经成功恢复出厂值。重启 HiPER 后，就可以通过局域网端口登录 WEB 管理界面（默认

IP 地址：192.168.16.1；用户名 Default；密码为空）。

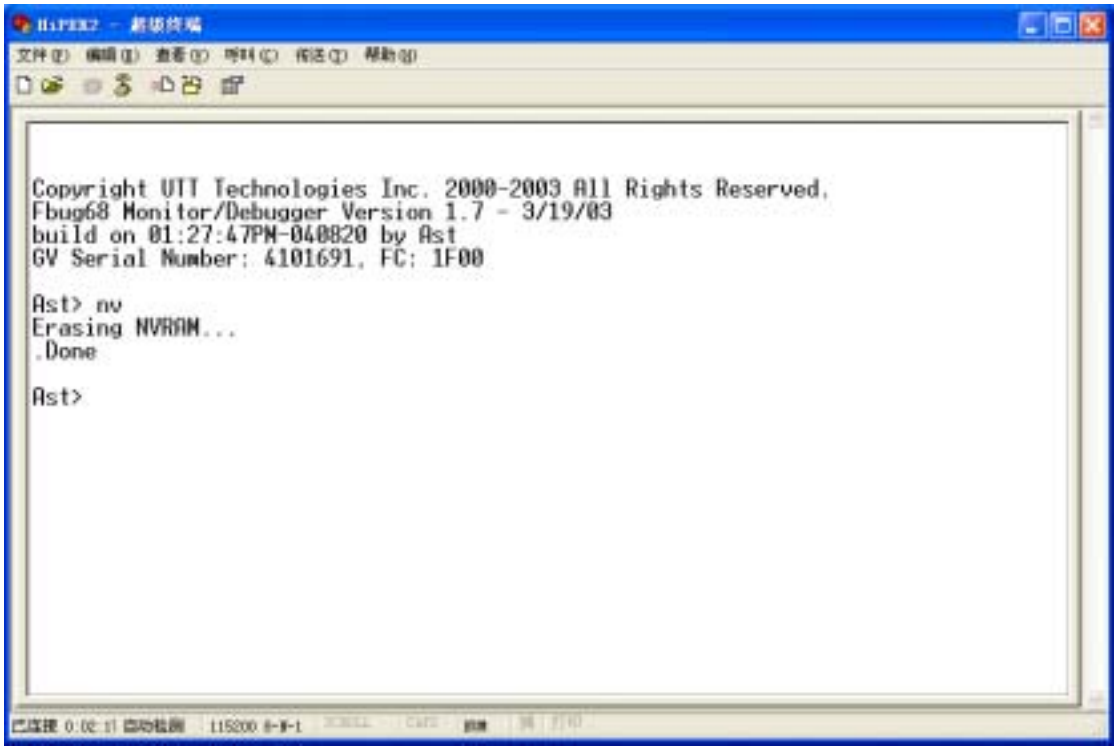


图 B-16 恢复出厂配置界面二（115200）

5．如何使用 CLI“急救模式”？

在 HiPER 中，我们将系统正常启动时使用的模式称为“正常启动模式”。

然而由于某些原因，比如因配置出现问题导致系统正常启动失败，或者因忘记管理员密码导致无法进入配置界面，系统将无法进入“正常启动模式”。为了解决这个问题，从 ReOS 5.0 开始，增加了“急救模式”。

进入“急救模式”后，系统将不再使用用户配置，而是直接以工厂缺省配置恢复系统，好比是台没有配置过的新设备一样；进入该模式后，可使用所有 CLI 命令，执行任何操作。

进入“急救模式”的步骤如下：

1) 首先，将随机附带的配置线一端（RJ45 接头）接入 HiPER 的 TERMINAL 接口，另一端（DB9 接头）接入计算机的串口。
2) 单击“开始”→“程序”→“附件”→“通讯”→“超级终端”（如果没有安装这个工具，请选择“我的电脑”→“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”→“通讯”，然后安装这个程序）。
3) 如图 B-17 所示，在“名称”中填入“rescue”，单击“确定”按钮。

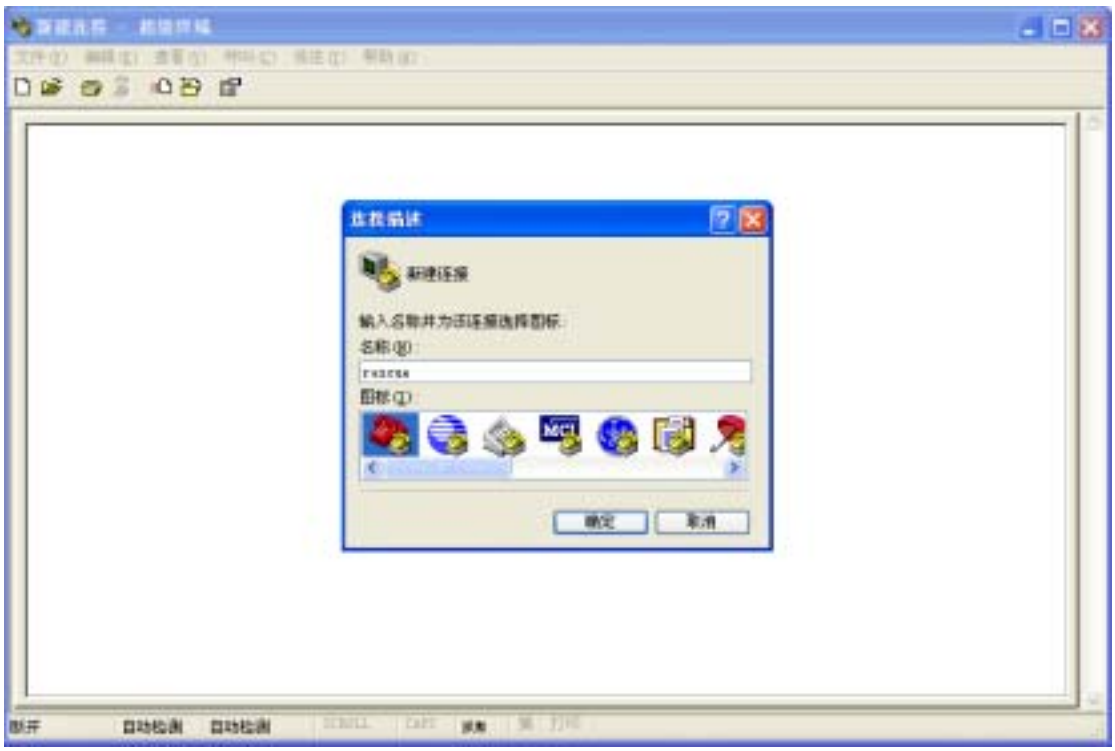


图 B-17 新建连接界面（rescue）

4) 如图 B-18 所示，在“ 选择连接时使用 ”中选择 COM X（根据实际情况选择配置线实际连接的计算机的串口），单击“ 确定 ”按钮。

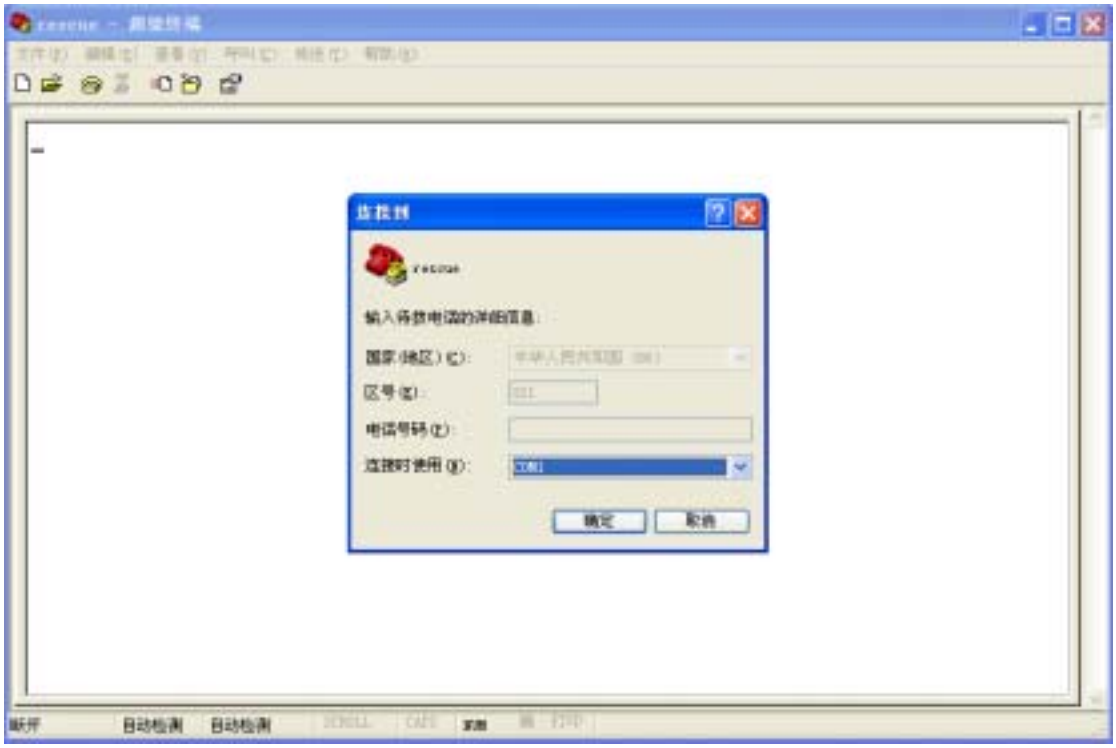


图 B-18 选择串口界面（rescue）

5) 如图 B-19 所示，选择“ 每秒位数 ”：9600；“ 数据位 ”：8；“ 奇偶校验 ”：无；“ 终止位 ”：1；“ 数据流控制 ”：无，单击“ 确定 ”按钮。

图 B-19 COM 口属性配置界面（rescue）

6) 进入如图 B-20 所示超级终端主控界面，此时需重启 HiPER。

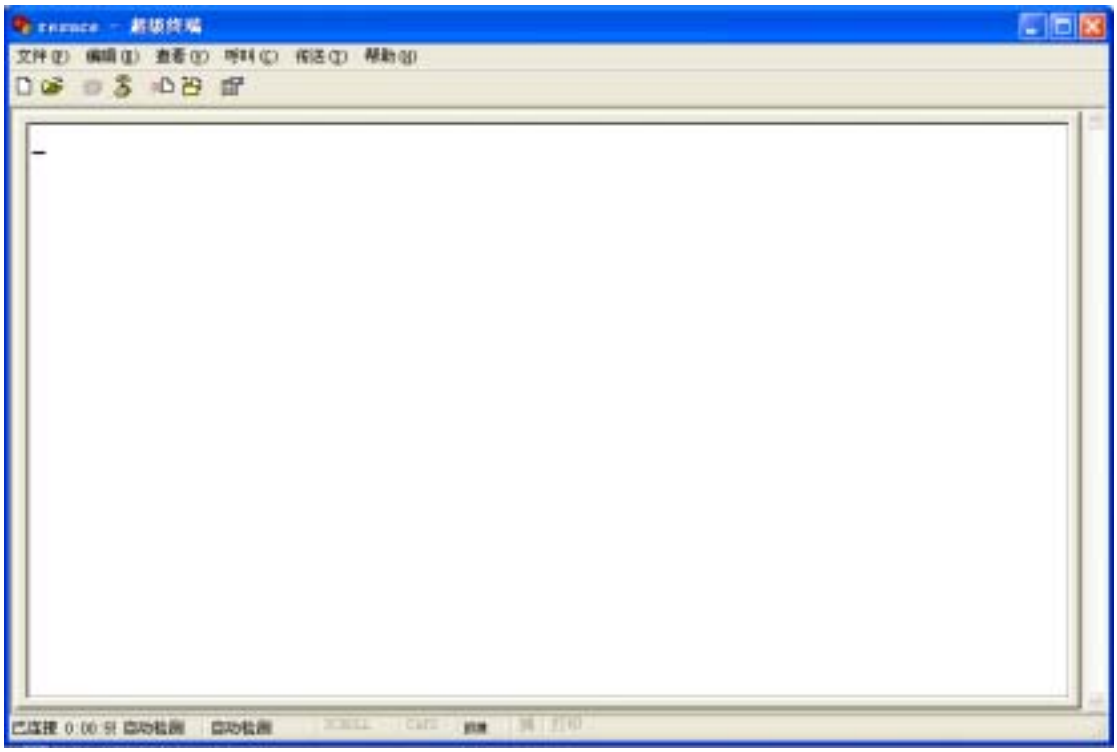


图 B-20 主控界面（rescue）

7) 如图 B-21 所示，当 HiPER 重启过程中，系统启动进入 REOS 引导阶段后，当看到“**Inflate begin.....OK** ”这行字符时，在 3 秒钟内连续输入三次<ctrl＋c>键。注意，一定要看到“ OK ”消息后再输入。

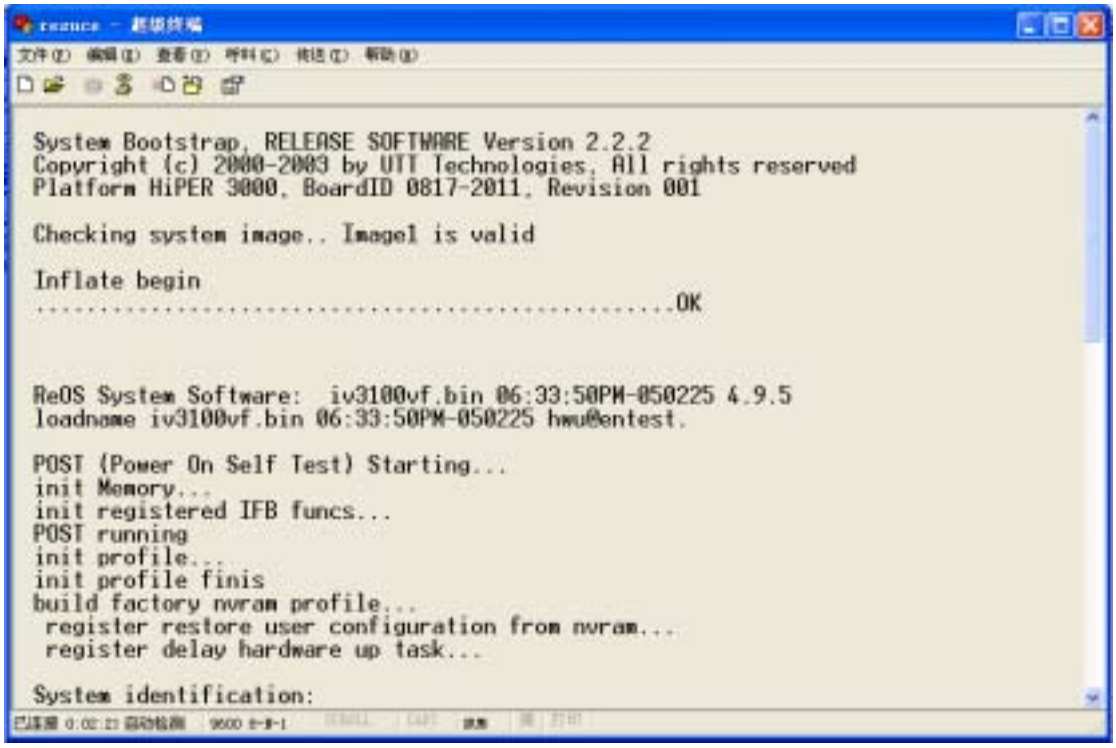


图 B-21 系统启动界面

8) 如图 B-22 所示，当成功进入“ 急救模式 ”后，系统会显示提示信息“ **BREAK detected, skip restore user nvram profile by _restoreUserNvramTask.** ”

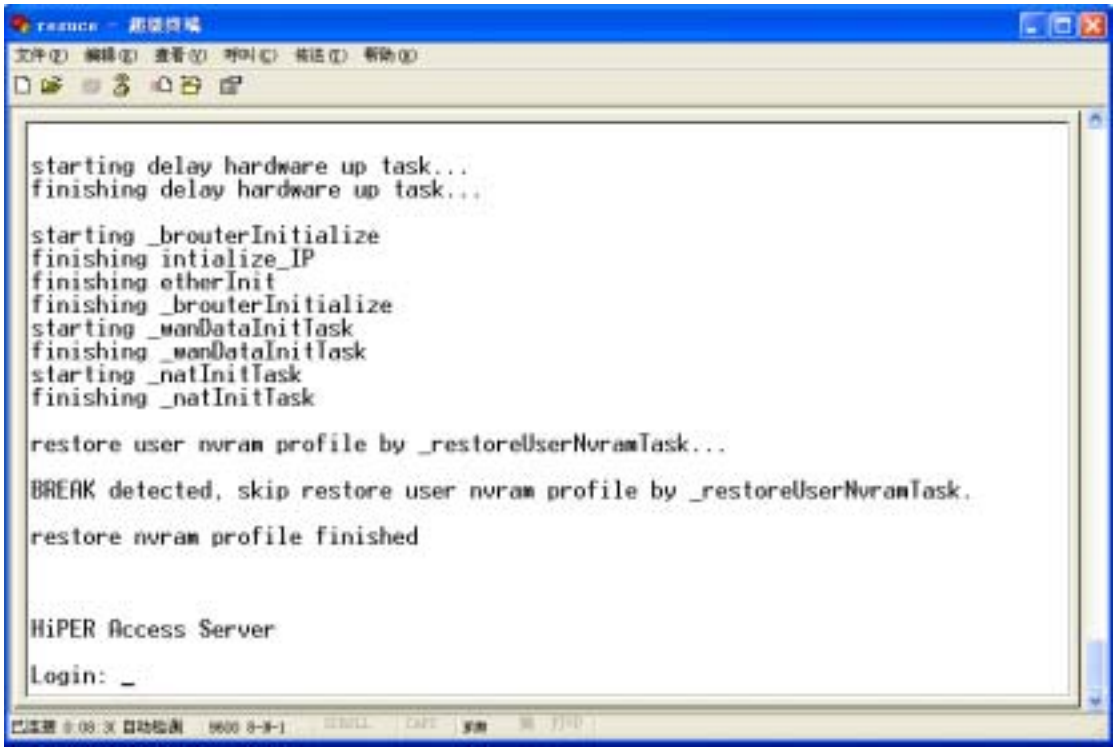


图 B-22 登录界面（rescue）

9) 如图 B-23 所示，进入“ 急救模式 ”后，使用出厂的管理员用户名/密码即可登录。在“ Login： ”后输入：Default<回车>，出现“ Password ”后，直接输入<回车>，将出现提示符“ rescue＃ ”，表示已进入“ 急救模式 ”配置界面。之后，即可进行任何操作。

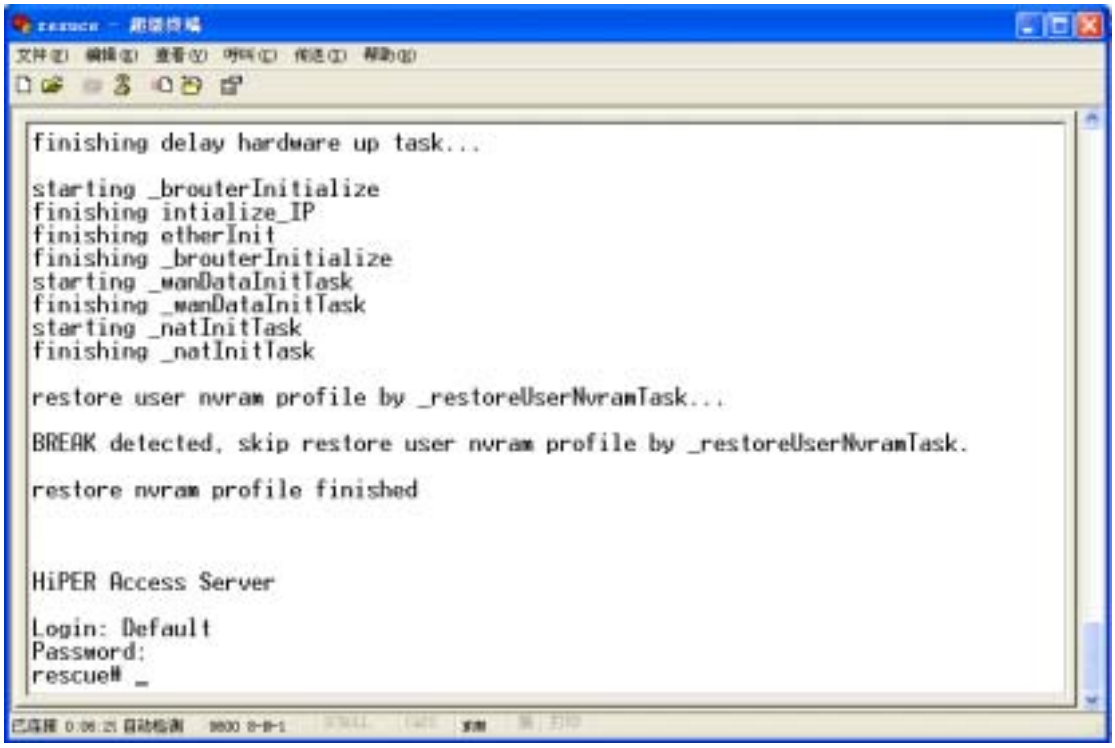


图 B-23 急救模式界面（rescue）

10) 如图 B-24 所示，在急救模式下，输入命令“ **show running** ”，输出为空，表明系统目前运行在出厂配置之下；输入命令“ **show nvram** ”，可看到用户的原有配置。

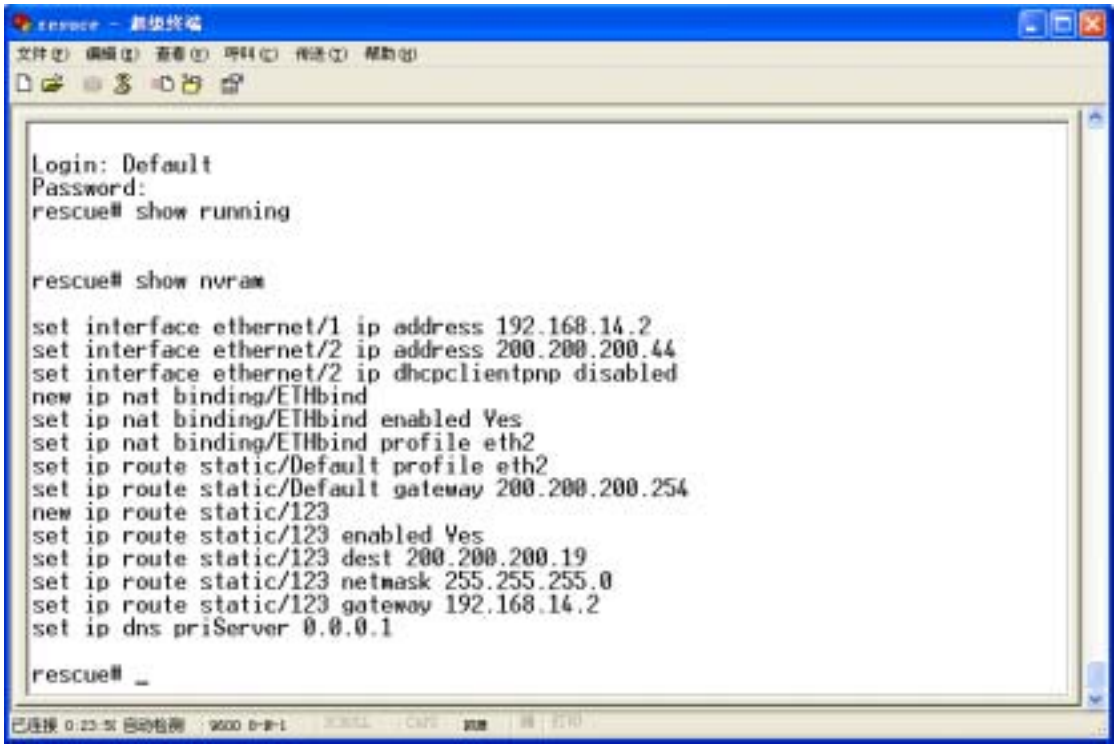


图 B-24 查看配置（rescue）

提示：在“ 急救模式 ”下，使用“ write ”命令后，只能保存执行本次命令前重新输入的配置信息，用户原先的所有配置将丢失。因此，如果需要保存用户的原有配置，就应当先输入“ **show nvram** ”以显示用户原先的所有配置，然后将需要的配置重新输入一遍（利

用拷贝、粘贴功能），最后才能执行“ write ”命令；或者在执行“ write ”命令之前，将用户需要保存的配置另存为文本文件，在进入“ 正常启动模式 ”后再将配置写入。

11) 最后需重新启动 HiPER，方可退出“ 急救模式 ”配置界面。

6. 用户管理（IP/MAC 绑定）、工作组与业务管理

本节主要讲述 HiPER 中，用户管理（IP/MAC 绑定）、工作组与业务管理三者的特点及其关系，目的是帮助大家更好地理解它们，并灵活地利用它们实现对用户上网行为的控制、加强网络的安全性。

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权（IP 业务管理）工作。在 HiPER 中，通过用户管理功能解决用户的身份识别问题，通过业务管理功能实现对用户上网行为的控制。

A. 用户管理

在用户管理中，通过 IP/MAC 地址绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址作为用户唯一的身份识别标识，可以防止 IP 地址盗用、MAC 地址盗用以及 IP/MAC 欺骗等常见攻击。

对于没有明确身份鉴别要求（即没有进行 IP/MAC 地址绑定）的用户，系统默认的用户全局策略是允许访问。如果将此策略设为禁止，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 6.5.2）中，不选中“ 允许非 IP/MAC 绑定用户 ”，那么将会拒绝所有身份无法识别的用户使用 HiPER。

用户管理功能只能影响用户访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该 HiPER 的通信）。也就是说，如果 IP/MAC 绑定用户修改了 IP 或 MAC，将不能访问 HiPER 或通过 HiPER 访问其他网络（如 Internet），但是不能影响局域网内部通信，比如网络邻居浏览。

B. 工作组

若干上网要求相同的局域网用户构成一个工作组，一个工作组通常包括多个 IP 地址连续的用户。这里，允许定义只有一个用户（工作组的起始 IP 地址和结束 IP 地址相同）的特殊工作组，我们将之称为个人用户。

C. 业务管理

在业务管理中，通过定义工作组、业务端口、协议、时间段等元素来实现对局域网中各工作组用户上网行为的控制，设置各工作组用户的各种上网权限和时间。

D. 三者关系

1) 用户管理只能完成用户身份识别、不能控制用户上网行为，用户上网行为的控制是通过业务管理功能完成的；
2) 工作组由若干上网要求相同的用户组成；
3) 业务管理功能是一般是针对工作组用户创建业务策略来实现的，同一个工作组的用户的上网权限完全相同，从而，你只需为工作组定义业务策略，而无需为每个用户分别定义业务策略。同时，如有需要，也可针对个人用户创建业务策略；
4) 在 HiPER 中，首先通过用户管理（IP/MAC 绑定）功能解决用户身份识别问题，然后将上网业务要求相同的用户划分在同一个工作组中，再通过对工作组用户（及个人用户）定义不同的业务策略。这样，不仅实现了对用户身份的识别，还实现

了对用户上网行为（包括上网权限和时间）的控制，从而保证了网络资源的有效利用及网络的安全性。

E. 功能实现过程

当用户有数据流量通过 HiPER 时，顺序发生以下动作：

1) 用户身份识别
   a) 如果是合法用户通过，该数据包进入 IP 业务管理处理；
   b) 如果用户身份不合法，丢弃该数据包；
   c) 如果用户身份未知，根据系统的用户全局策略执行：
      i. 若允许未知用户，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 6.5.2）中，选中“ 允许非 IP/MAC 绑定用户 ”时，让该数据包通过，进入 IP 业务管理处理；
      ii. 若禁止未知用户，即在 ***WEB 管理界面—>高级配置—>用户管理—>用户管理全局设置***（章节 6.5.2）中，禁用“ 允许非 IP/MAC 绑定用户 ”时，丢弃该数据包。

提示：合法用户指，其 IP 地址和 MAC 地址与“ 用户绑定信息列表 ”（参见 ***WEB 管理界面—>高级配置—>用户管理—>用户绑定信息列表***〈章节 6.5.3〉）中的某条目的 IP 地址和 MAC 地址完全匹配；不合法用户指，其 IP 地址和 MAC 地址中只有一个与“ 用户绑定信息列表 ”（参见 ***WEB 管理界面—>高级配置—>用户管理—>用户绑定信息列表***〈章节 6.5.3〉）中的某条目的 IP 地址或 MAC 地址匹配，另一个则不匹配；身份未知用户指，合法用户和不合法用户之外的所有用户。

2) 业务管理处理流程（包括时间段控制）

HiPER 将从“ 业务策略信息列表 ”（参见 ***WEB 管理界面—>高级配置—> 业务管理—>业务策略信息列表***〈章节 6.2.4〉）的顶端开始向下搜索该表，查找第一个与数据包的源地址、目的地址、协议、目的端口、源端口以及接收到数据包请求的时间相匹配的策略。匹配的第一个策略将被应用于数据包，将不再检查后面的策略。如果没有找到匹配的策略，出于安全考虑，该数据包将被丢弃。

注意，对于设置了时间段的业务策略来说，首先还需判断该时间段是否是有效时间段。当时间段有效期已过，该时间段无效，将不再起作用；如果需要时间段策略控制，必须重新配置该时间段。

在启用了业务管理之后，系统会形成七种业务策略：

a) 为使 HiPER 正常工作而自动生成的名称为“ lan ”、“ dns ”以及“ dhcp ”的系统缺省业务策略，它们分别用来允许访问 LAN 口、允许 DNS、DHCP 服务；
b) 自定义的个人用户策略，可能是禁止或允许该用户的某项上网业务；
c) 自定义的工作组策略，可能是禁止或者允许该组的某项上网业务；
d) 系统自动生成的某工作组的全局策略，默认是禁止该组除定义过的其他业务。当为某工作组定义业务策略后，系统会自动生成该组的全局策略，名称为“ grpx_other ”，x 为阿拉伯数字，按照配置顺序依次为 1、2、3……；
e) 自定义的系统默认（IPSSG）组策略，可能是禁止或者允许 IPSSG 组的某项上网业务，但是该组的源起止 IP 地址不能修改；
f) 系统自动生成的 IPSSG 组的全局策略，默认是允许 IPSSG 组除定义过的其他业务，该业务策略的名称为“ pass ”。可在 ***WEB 管理界面—>高级配置—>业务管理—>业务管理全局配置***（章节 6.2.3）中，通过设置“ 允许其它用户 ”来指定其“ 动作 ”，默认是选中，表示允许；

g) 系统自动生成的全局策略（作用于局域网所有用户），允许所有数据包（包括其他非 IP 类型的包）通过，该业务策略的名称为“ generic ”。

一般情况下，在“ 业务策略信息列表 ”中，其中，业务策略按照从上到下的顺序依次是：**“ lan ”、“ dns ”及“ dhcp ”**这 3 条策略**——>自定义的个人用户策略——>自定义的工作组策略（包括工作组全局策略）——>自定义的 IPSSG 组策略——>“ pass ”和“ generic ”**这 2 条策略。需要指出的是，“ lan ”、“ pass ”及“ generic ”这 3 条系统自动生成的策略未在“ 业务策略信息列表 ”中显示。

对于工作组策略来说，缺省情况下，工作组策略将按照配置时的顺序从上到下依次排列，自定义的工作组策略将自动位于该组全局策略上方，但用户可以通过参数“ 插入位置 ”指定或调整某工作组策略的位置，并且，只能是在某工作组内部或工作组之间调整。注意，如果将某条自定义的工作组策略插入到该工作组全局策略下方，这条策略将不再起作用。

对于个人用户策略来说，缺省情况下，个人用户策略将按照配置时的顺序从上到下依次排列，但用户可以通过参数“ 插入位置 ”指定或调整某个人用户策略的位置，并且，只能在个人用户策略之间调整。

F. 自定义用户身份及其业务权限

由以上分析可知，如果要配置一个局域网的用户及其上网的业务权限，就应该遵循以下步骤：

1） 规划局域网每个用户，确定用户是否拥有连接和通过 HiPER 的权限，以及这些用户上网所能使用的权限；
2） 将上网权限相同的用户合并，将局域网用户划分成若干个 IP 地址连续的工作组；
3） 根据上一步的规划为每个用户的计算机设置 TCP/IP 属性，并且记录下每个用户的 MAC 地址；
4） 在 ***WEB 管理界面—>高级配置—>用户管理***（章节 6.5）中，配置 IP 和 MAC 绑定（如果要禁止非允许的 IP/MAC 绑定用户连接和通过 HiPER，请取消“ 允许非 IP/MAC 绑定用户 ”的选中）；
5） 在 ***WEB 管理界面—>高级配置—>组管理—>工作组配置***（章节 6.1.1）中，配置工作组；
6） 在 ***WEB 管理界面—>系统管理—>时钟管理***（章节 5.2）中，校正 HiPER 当前系统时间；
7） 如果要限制用户的上网时间，在 ***WEB 管理界面—>基本配置—>时间段配置—>自定义时间段***（章节 4.6.3）中，配置时间段；
8） 在 ***WEB 管理界面—>高级配置—>业务管理—>业务策略配置***（章节 6.2.2）中，配置每个工作组的上网权限（如果只允许已配置了上网权限的工作组上网，请取消“ 允许其它用户 ”的选中）；
9） 配置完毕后，还可以在 ***WEB 管理界面—>带宽业务***（章节 9）中，配置各工作组上网的下行带宽。

7．怎样使用 NetMeeting 聊天？

1) 如果是局域网主机发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。
2) 如果希望能接收来自对方的 NetMeeting 呼叫，则需要设置 NAT 静态映射或者虚拟服务器（DMZ 主机）。

3) 设置 NAT 静态映射的方法：在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 静态映射配置***（章节 6.3.4）中，设置 NAT 静态映射，如图 B-25 所示：

首先选择“ 添加 ”选项，然后在“ NAT 静态映射名 ”中填入 netmeeting（可自定义），“ 协议 ”选择 TCP，在“ 外部起始端口 ”中填入 1720，在“ 内部起始端口 ”中填入 1720，在“ 内部 IP 地址 ”中填入 192.168.16.221（假设计算机的 IP 地址是 192.168.16.221），单击“ 保存 ”按钮，设置完成。

图 B-25 NAT 静态映射（Netmeeting）配置

提示：局域网同时只允许一台计算机做 1720 端口的 NAT 静态映射。

4) 设置虚拟服务器（DMZ）的方法：在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置***（章节 6.3.2）中，设置虚拟服务器（DMZ），如图 B-26 所示：

在“ 虚拟服务器（DMZ）”中填入 192.168.16.221（假设计算机的 IP 地址是 192.168.16.221），单击“ 保存 ”按钮，设置完成。

图 B-26 虚拟服务器（DMZ）配置

8. 怎样发现使用带宽最大的用户？

HiPER 提供了查看系统状态功能，可以在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，即可发现使用带宽最大的用户。

A. 发现下载量最大的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询“ 下载数据包/总数 ”，该百分比值越大，就表示下载数据包数量越多，该数值最大的用户就是局域网中通过 Internet 下载量最大的用户。

B. 发现上传量最大的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询“ 上传数据包/总数 ”，该百分比值越大，就表示上传数据包数量越多，该数值

最大的用户就是局域网中通过 Internet 上传量最大的用户。

C. 发现上网最活跃的用户

在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，“ 查看 NAT 统计信息列表 ”，查询“ 当前连接数/总数 ”，该百分比值越大，就表示用户上网越活跃，该数值最大的用户就是局域网中当前上网最活跃的用户。

9. 怎样诊断蠕虫病毒或者黑客攻击造成的 HiPER 使用异常的故障？

提示：以下各点仅在排除网络故障时作为参考，不作为发现网络病毒或各种攻击的依据。

A. 发现内部用户使用地址扫描软件扫描 Internet

【地址/端口扫描软件】在使用此类软件时，软件会在单位时间向目标地址或者目标网段发出大量的 ICMP/UDP 包或者 TCP 连接，以扫描目标地址是否存在或者是否有开放的端口。使用这些软件的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点 HiPER 负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以通过以下 3 种方式找出使用地址/端口扫描软件的用户。

1) 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有 “ 超限次数 ”大于 100 的用户。由于 HiPER 支持用户在单位时间内最多只能有 800 条 NAT 连接（这完全能保障正常上网的用户），超过的连接将被 HiPER 丢弃，并在“ 超限次数 ”里面增加记录，因而当“ 超限次数 ”大于 100 时，该用户很可能正在使用地址/端口扫描软件。
2) 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息列表 ”，查询是否有“ 上传数据包 ”数量比“ 下载数据包 ”数量大很多的用户。由于地址/端口扫描软件在往外发送数据包的时候，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回的发送方，因而当某用户“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量时，该用户很可能正在使用地址/端口扫描软件。
3) ***在 WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.6.3）中，查看系统历史记录，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded 192.168.16.221 ”），表示该 IP 地址的计算机 NAT 并发 session 超过了 HiPER 限定的最大 session 数，则该用户很可能正在正在使用地址/端口扫描软件。

   提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

B. 发现局域网用户使用 DoS/DDos 方式攻击 Internet 主机

【DoS/DDoS 攻击】俗称洪水攻击、术语称拒绝服务攻击或称分布性拒绝访问。这种攻击方法在很短的时段内向某一网站发出大量信息，使其超出该网站自身的负荷能力而“ 无法对用户提供正常服务 ”，造成网站业务不能正常开展。使用这些攻击方式的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点 HiPER 负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以根据以下方法找出使用地址/端口扫描软件的用户。

1) 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看“ NAT 统计信息

列表 ”，查询是否有 “ 上传数据包 ” 数量比其他用户大很多、“ 下载数据包 ” 数量却很少的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，会向 Internet 发送大量的数据包，因此如果某用户的 “ 上传数据包 ” 数量比其他用户大很多、“ 下载数据包 ” 数量却很少，那么该用户很可能正在进行 DoS/DDoS 攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

2) 在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看 “ NAT 统计信息列表 ”，查询是否有 “ 上传数据包 ” 数量比 “ 下载数据包 ” 数量大很多的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回的发送方，因而当某用户“ 上传数据包 ”数量远远大于“ 下载数据包 ” 数量时，该用户很可能正在进行 DoS/DDoS 攻击。

3) ***在 WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.6.3）中，查看系统历史记录，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded 192.168.16.221 ”），表示该 IP 地址的计算机 NAT 并发 session 超过了 HiPER 限定的最大 session 数，则该用户很可能正在进行 DoS/DDoS 攻击。

提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

C. 发现 RED_WORM（红色代码 Code red）类型的网络攻击型病毒

1) 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有 “ 发送数据包 ” 数量很大的用户；同时在 ***WEB 管理界面—>系统状态—>NAT 统计***（章节 7.2.2）中，查看 “ NAT 统计信息列表 ”，查询是否有 “ 下载数据包 ” 数量很小或没有的用户。如果某用户同时满足上述条件，同时该用户也未使用过局域网中的各种服务器，则该用户很可能正在已经感染上 RED_WORM 类型的网络攻击型病毒。

2) 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有 “ 发送广播包 ” 数量很大，大于其 “ 发送数据包 ” 数量的 10%的用户。如果某用户 “ 发送广播包 ” 数量与 “ 发送数据包 ” 数量的百分比大于 10%，则该用户很可能已经感染上 RED_WORM 类型的网络攻击型病毒。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

D. 发现 TCP SYN FLOOD，UDP FLOOD，ICMP FLOOD 类型的网络攻击

在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有 “ 发送数据包 ” 数量很大、“ 接收数据包 ” 数量很小的用户。如果某用户 “ 发送数据包 ” 数量很大，同时 “ 接收数据包 ” 数量很小，则该用户很可能正在进行 TCP SYN FLOOD、UDP FLOOD 或 ICMP FLOOD 类型的攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

E. 发现 ARP FLOOD 类型的网络攻击

1) 在 ***WEB 管理界面—>系统状态—>用户统计***（章节 7.1）中，查看“ 用户统计信息列表 ”，查询是否有 “ 发送广播包 ” 数量很大，大于其 “ 发送数据包 ” 数量的 10%的用户。如果某用户 “ 发送广播包 ” 数量与 “ 发送数据包 ” 数量的百分比大于 10%，则该用户很可能正在进行 ARP FLOOD 型攻击。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

2) 在 ***WEB 管理界面—>系统状态—>系统信息—>系统历史记录***（章节 7.6.3）中，查看系统历史记录，如果发现某 IP 地址的 MAC 地址经常变化（例如显示出信息“ MAC CHGED 192.168.16.221 ”、“ MAC OLD 00:22:AA:00:22:AA ”以及“ MAC NEW 00:22:AA:00:22:BB ”），则该用户很可能正在进行 ARP FLOOD 型攻击。

F. 发现冲击波/震荡波等蠕虫病毒攻击

感染了“ 冲击波 ”、“ 震荡波 ”病毒的个人电脑会随机向外发送大量的 ICMP 包以及向目的端口为 135/137/139/445 的端口发送大量的广播包，造成 HiPER 端口拥塞，直至整个内部网络、外部网络的瘫痪。

在 ***WEB 管理界面—>上网监控***（章节 8.2）中，“ 选择查看条件 ”为“ 全部记录 ”，查看“ 查询结果列表 ”，如果在全部“ 协议类型 ”一列中，发现很多类型为 ICMP 的条目；在“ 外网端口 ”一列中，发现很多端口为 135/137/139/445 的条目，这些条目占用了大量的 NAT Seesion 条目，则很可能有主机感染了“ 冲击波 ”、“ 震荡波 ”病毒。

“ 冲击波 ”病毒感染计算机之后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；IE 浏览器不能正常地打开链接；不能复制粘贴；有时出现应用程序，比如 Word 异常；网络变慢；在任务管理器里有一个叫“ msblast.exe ”的进程在运行。

“ 震荡波 ”病毒感染计算机后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；任务管理器里有一个叫“ avserve.exe ”、“ avserve2.exe ”或者“ skynetave.exe ”的进程在运行；在系统目录下，产生一个名为 avserve.exe、avserve2.exe、skynetave.exe 的病毒文件；系统速度极慢，CPU 占用 100%。

10. 怎样实现允许从外网 ping 广域网端口地址？

为了方便诊断和测试的需要，HiPER 允许从外网 Ping 广域网端口地址，以检测线路连接是否正常。实现方法如下：在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置***（章节 6.3）中，将内网中的一台主机设置为“ 虚拟服务器 ”（即 DMZ 主机）即可。

配置完成之后，在该虚拟服务器工作正常情况下，从外网执行 ping 命令，如果能 ping 通当前 WAN 口或 WAN2/DMZ 口的 IP 地址，则表示主线路或备份线路连接正常；如果不能 ping 通当前 WAN 口或 WAN2/DMZ 口的 IP 地址，则表示主线路或备份线路连接异常，可能是线路本身有问题，或者是线路中某处设备不转发 ICMP 包（禁 ping），也有可能是 HiPER 配置有问题，等等。

提示：

1) 执行 ping 命令时，需保证虚拟服务器工作正常，否则将无法 ping 通 WAN 口（或 WAN2/DMZ 口）地址，这样可能会错误认为该线路连接不正常；

2) 被设置为虚拟服务器的计算机将失去 HiPER 的防火墙保护功能。

方法一 配置局部虚拟服务器（DMZ）

在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 规则***（章节 6.3.3）中，只要在主线路 NAT 规则中设置“ 虚拟服务器 ”，HiPER 就允许从外网对 WAN 口执行 ping 命令；同样地，只要在备份线路 NAT 规则中设置“ 虚拟服务器 ”，HiPER 就允许从外网对 WAN2/DMZ 口执行 ping 命令。

例如：如图 B-27 所示，假设欲作为服务器的 IP 地址为 192.168.16.20，如果希望从外网对 WAN 口执行 ping 命令，则只需在主线路 NAT 规则的“ 虚拟服务器 ”中填入 192.168.16.20，再单击“ 保存 ”按钮，配置完成。

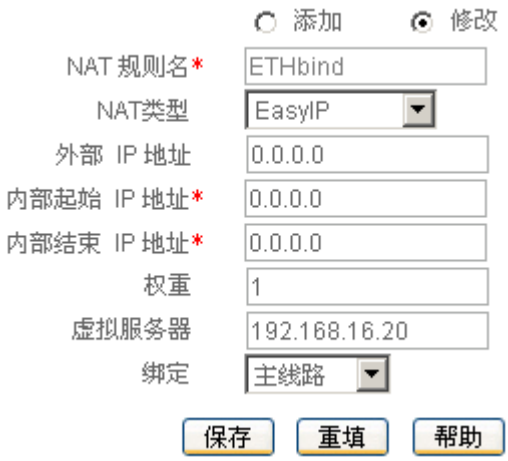


图 B-27 局部虚拟服务器（DMZ）配置

方法二 配置全局虚拟服务器（DMZ）

在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 全局配置***（章节 6.3.2）中，只要设置全局虚拟服务器，HiPER 就允许从外网对 WAN 口和 WAN2/DMZ 口执行 ping 命令。

例如：如图 B-28 所示，假设欲作为 DMZ 主机的 IP 地址为 192.168.16.10，则只需在“虚拟服务器（DMZ）”中填入 192.168.16.10，再单击“保存”按钮，配置完成。

图 B-28 全局虚拟服务器（DMZ）配置

提示：由于局部虚拟服务器的优先级比全局虚拟服务器高，建议在 ***WEB 管理界面—>高级配置—>NAT 和 DMZ 配置—>NAT 规则***（章节 6.3.3）中没有为主线路 NAT 规则和备份线路 NAT 规则设置“虚拟服务器”时，使用本方法。否则，执行 ping 命令时，必须保证已设置的局部虚拟服务器工作正常，从而避免错误地认为线路失效。

附录 C 常用 IP 协议

协议	协议号	全称
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Porotocl
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocl
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhandced Interior Gateway Routing Portocol
OSPF	89	Open Shortest Path First

附录 D 常用服务端口

服务	端口号	协议	描述
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client

tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol

ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	
conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	

remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

附录 E　图索引

图 0-1 DNS 服务器配置 4
图 0-2 启用快速转发 4
图 2-1 建立局域网和广域网连接——HiPER 3110 SOHO/3110/2190NBII 11
图 2-2 前面板指示灯示意图——HiPER 3110 SOHO/3110/2190NBII 12
图 2-3 后面板指示灯示意图——HiPER 3110 SOHO/3110/2190NBII 12
图 2-4 建立局域网和广域网连接——HiPER 2231CS/2190NB+ 13
图 2-5 前面板指示灯示意图——HiPER 2231CS/2190NB+ 14
图 3-1 HiPER 登录界面 16
图 3-2 WEB 界面首页 17
图 3-3 登录密码设置 17
图 3-4 系统时钟设置 18
图 3-5 上网接入方式设置 18
图 3-6 PPPoE 拨号上网方式 19
图 3-7 PPPoE 拨号配置 20
图 3-8 固定 IP 接入方式 21
图 3-9 固定 IP 接入配置 21
图 3-10 动态 IP 接入方式 22
图 3-11 动态 IP 接入配置 22
图 4-1 PPPoE 拨号时线路连接信息 25
图 4-2 固定 IP 接入时线路连接信息 27
图 4-3 动态 IP 接入时线路连接信息 28
图 4-4 双线路接入时线路连接信息 29
图 4-5 选择线路和连接类型 30
图 4-6 PPPoE 拨号配置 31
图 4-7 固定 IP 接入配置 33
图 4-8 动态 IP 接入配置 33
图 4-9 删除主线路（和备份线路） 34
图 4-10 对话框——删除主线路 35
图 4-11 对话框——删除主线路和备份线路 35
图 4-12 删除备份线路 35
图 4-13 对话框——删除备份线路 35
图 4-14 线路组合配置——线路备份 38
图 4-15 线路组合配置——负载均衡 41
图 4-16 线路组合配置——实例 42
图 4-17 调度规则配置 44
图 4-18 DHCP 服务配置 46
图 4-19 DHCP 手工绑定配置 48
图 4-20 端口配置 50
图 4-21 DDNS 服务配置 54

图 4-22 DDNS 状态 54
图 4-23 对话框——请先配置 PPPoE 55
图 4-24 DDNS 状态 56
图 4-25 时间段配置 57
图 4-26 时间段详细信息 59
图 4-27 时间段配置——实例 60
图 5-1 管理员配置 62
图 5-2 时钟管理配置 64
图 5-3 显示和保存当前软件 65
图 5-4 软件升级 65
图 5-5 保存配置 67
图 5-6 恢复备份配置 67
图 5-7 恢复出厂配置 67
图 5-8 重新启动设备 68
图 5-9 WEB 服务器配置 68
图 5-10 SNMP 配置 69
图 5-11 SYSLOG 配置 70
图 5-12 远程管理 71
图 6-1 工作组配置 72
图 6-2 工作组 Sale 配置 74
图 6-3 工作组 Technique 配置 74
图 6-4 工作组 Admin 配置 74
图 6-5 业务策略配置 78
图 6-6 启用业务管理 79
图 6-7 源端口的应用实例 86
图 6-8 NAT 全局配置 90
图 6-9 NAT 规则配置——EasyIP 91
图 6-10 NAT 规则配置——One2One 92
图 6-11 NAT 规则配置——Passthrough 92
图 6-12 NAT 规则配置——实例一 95
图 6-13 NAT 规则配置实例方案图——One2One 方式 96
图 6-14 NAT 规则配置——实例二 97
图 6-15 NAT 规则配置实例方案图——Passthrough 方式 97
图 6-16 NAT 规则配置——实例三 98
图 6-17 NAT 静态映射配置 99
图 6-18 NAT 静态映射配置——实例一 101
图 6-19 NAT 静态映射配置——实例二 101
图 6-20 NAT 静态映射配置——实例三 102
图 6-21 静态路由配置 104
图 6-22 路由参数设置——实例一 106
图 6-23 路由参数设置——实例二 106
图 6-24 IP 和 MAC 地址绑定用户配置 109
图 6-25 ARP 表信息 109
图 6-26 IP 和 MAC 地址绑定用户配置——实例 1 109

图 6-27 用户管理全局设置 110
图 6-28 启用快速转发 113
图 6-29 内网主机速率限制 114
图 6-30 虚拟局域网 114
图 6-31 启用端口镜像 115
图 6-32 端口镜像应用 115
图 7-1 系统版本信息 126
图 7-2 系统运行时间 126
图 7-3 系统历史记录 127
图 7-4 系统异常信息 129
图 8-1 选择查询条件 130
图 8-2 选择查询条件——实例一 132
图 8-3 选择查询条件——实例二 132
图 8-4 选择查询条件——实例三 133
图 8-5 选择查询条件——实例四 134
图 8-6 查询条件——实例五 134
图 8-7 查询条件——实例六 135
图 9-1 带宽管理基本信息配置 136
图 9-2 带宽管理策略配置 137
图 9-3 带宽管理策略配置（Technique） 140
图 9-4 带宽管理策略配置（Admin） 140
图 9-5 带宽管理策略配置(Other) 140
图 A-1 网络配置窗口 141
图 A-2 TCP/IP 属性 IP 地址配置窗口 142
图 A-3 TCP/IP 属性网关配置窗口 143
图 A-4 TCP/IP 属性 DNS 配置窗口 143
图 A-5 TCP/IP 属性 IP 地址配置窗口 144
图 A-6 TCP/IP 属性网关配置窗口 145
图 A-7 TCP/IP 属性 DNS 配置窗口 145
图 B-1 PPPoE 拨号主线路连接信息 147
图 B-2 PPPoE 拨号配置（部分） 148
图 B-3 动态 IP 接入时主线路连接信息 149
图 B-4 新建连接界面（9600） 150
图 B-5 选择串口界面（9600） 151
图 B-6 COM 口属性配置界面（9600） 151
图 B-7 主控界面（9600） 152
图 B-8 登录界面一（9600） 152
图 B-9 登录界面二（9600） 153
图 B-10 恢复出厂配置界面（9600） 153
图 B-11 新建连接界面（115200） 154
图 B-12 选择串口界面（115200） 155
图 B-13 COM 口属性配置界面（115200） 155
图 B-14 主控界面（115200） 156
图 B-15 恢复出厂配置界面一（115200） 156

图 B-16 恢复出厂配置界面二（115200） 157
图 B-17 新建连接界面（rescue） 158
图 B-18 选择串口界面（rescue） 158
图 B-19 COM 口属性配置界面（rescue） 159
图 B-20 主控界面（rescue） 159
图 B-21 系统启动界面 160
图 B-22 登录界面（rescue） 160
图 B-23 急救模式界面（rescue） 161
图 B-24 查看配置（rescue） 161
图 B-25 NAT 静态映射（Netmeeting）配置 165
图 B-26 虚拟服务器（DMZ）配置 165
图 B-27 局部虚拟服务器（DMZ）配置 169
图 B-28 全局虚拟服务器（DMZ）配置 169

附录 F　表索引

表 0-1 手册适用产品一览表 1
表 0-2 DHCP 手工绑定信息列表 2
表 0-3 DHCP 地址池使用信息列表 3
表 0-4 端口出厂配置 4
表 2-1 前面板指示灯状态——HiPER 3110 SOHO/3110/2190NBII 12
表 2-2 后面板指示灯状态——HiPER 3110 SOHO/3110/2190NBII 12
表 2-3 前面板指示灯状态——HiPER 2231CS/2190NB+ 14
表 2-4 后面板指示灯状态——HiPER 2231CS/2190NB+ 14
表 4-1 PPPoE 拨号线路连接状态描述 25
表 4-2 固定 IP 接入线路连接状态描述 27
表 4-3 动态 IP 接入线路连接状态描述 28
表 4-4 各种检测方法支持的检测地址类型 37
表 4-5 路由表信息列表——实例一 43
表 4-6 路由表信息列表——实例二 43
表 4-7 路由表信息列表——实例三 43
表 4-8 DHCP 地址池使用信息 47
表 4-9 DHCP 手工绑定列表 49
表 4-10 动态域名注册表 53
表 4-11 DDNS 状态信息 55
表 4-12 时间段信息列表 58
表 5-1 管理员信息列表 63
表 6-1 组信息列表 73
表 6-2 工作组配置信息 74
表 6-3 业务策略类别及排列顺序 76
表 6-4 业务策略信息列表 80
表 6-5 业务策略信息列表（续表 6-4） 80
表 6-6 业务策略信息列表——实例一 82
表 6-7 业务策略信息列表（续表 6-6）——实例一 82
表 6-8 业务策略信息列表——实例二 83
表 6-9 业务策略信息列表（续表 6-8）——实例二 83
表 6-10 业务策略信息列表——实例三 84
表 6-11 业务策略信息列表（续表 6-10）——实例三 84
表 6-12 业务策略信息列表——实例四 85
表 6-13 业务策略信息列表（续表 6-12）——实例四 85
表 6-14 主线路（备份线路）NAT 规则名称 88
表 6-15 NAT 规则信息列表 93
表 6-16 NAT 静态映射列表 100
表 6-17 系统保留路由 104
表 6-18 路由信息列表 105
表 6-19 用户绑定信息列表——实例一 108

表 6-20 用户绑定信息列表 110
表 6-21 用户绑定信息列表——实例二 112
表 6-22 用户绑定信息列表——实例三 112
表 7-1 用户统计信息列表 116
表 7-2 NAT 状态信息列表 118
表 7-3 NAT 统计信息列表 119
表 7-4 NAT 统计信息列表（续表 7-3） 119
表 7-5 端口统计信息列表 121
表 7-6 端口统计信息列表（续表 7-5） 121
表 7-7 路由表信息列表 122
表 7-8 路由表信息列表（续表 7-7） 123
表 7-9 路由表信息列表——实例一 124
表 7-10 路由表信息列表——实例二 124
表 7-11 路由表信息列表——实例三 124
表 7-12 端口信息列表 125
表 7-13 系统版本信息描述 126
表 7-14 系统历史记录 128
表 8-1 查询结果列表 131
表 8-2 查询结果列表——实例一 132
表 8-3 查询结果列表——实例二 133
表 8-4 查询结果列表——实例三 133
表 8-5 查询结果列表——实例四 134
表 8-6 查询结果列表——实例五 134
表 8-7 查询结果列表——实例六 135
表 9-1 带宽业务列表 138
表 9-2 带宽业务配置信息 139
表 B-1 PPPoE 拨号历史记录 148
表 B-2 路由表信息列表——实例一 148
表 B-3 路由表信息列表——实例二 149
表 B-4 路由表信息列表——实例三 150